100 Common Non-Conformities in ISO/IEC 20000 Audits

Your Field Guide to Building a World-Class IT Service Management System (SMS)

Objectives of this Guide:

Achieving ISO/IEC 20000 certification is a powerful step toward delivering consistent, high-quality, and secure IT services.

But many organizations encounter roadblocks — not because they lack intent, but because of recurring, avoidable audit failures.

This guide helps you recognize and eliminate the most common gaps found in real-world ISO/IEC 20000 audits.

✓ Identify critical ISO 20000 non-conformities across service delivery, change management, SLAs, supplier control, and more
✓ Deliver structured, audit-ready solutions that align with ISO 20000:2018 clauses
✓ Use real-world examples to build practical awareness for IT teams and auditors
✓ Promote a culture of continual improvement in IT service management
✓ Streamline the audit process by closing gaps proactively, not reactively

This guide is ideal for:

- IT Service Managers, Delivery Leads, and Operations Teams preparing for ISO 20000 certification
- Internal Auditors and IT Governance Professionals conducting audits or pre-assessments

- Consultants and trainers leading ISO 20000 implementation projects
- Business leaders seeking to mature their ITSM capabilities through globally accepted best practices

1. Undefined or Incomplete SMS Scope

📌 Clause: 4.3 – Determining the Scope of the SMS

What's going wrong:
Organizations often fail to define the full scope of their Service Management System (SMS), omitting services, support teams, outsourced elements, or customer-facing platforms.

Why it matters during an ISO 20000 audit:
An unclear or overly narrow scope can mislead auditors and result in non-conformities. Without a precise scope, it's impossible to assess whether controls cover all applicable services.

How to fix it:
✓ Clearly define services, technologies, departments, and suppliers included in your SMS
✓ Document physical and logical boundaries
✓ Align scope with your service catalog and ensure stakeholder awareness
✓ Reassess scope after structural or service changes

Real-world result:
A well-defined scope enables better audit alignment, reduces service gaps, and creates confidence in the SMS.

2. No Formal Service Management Policy

📌 Clause: 5.2 – Service Management Policy

What's going wrong:
Many organizations operate ITSM processes without a documented, approved, and communicated service management policy.

Why it matters during an ISO 20000 audit:
The policy demonstrates top management commitment. Without it, auditors will flag the absence of strategic alignment and governance.

How to fix it:

✓ Draft a policy aligned with the organization's goals, customer needs, and SMS objectives

✓ Get executive approval and communicate it organization-wide

✓ Review and update the policy annually or when the SMS changes

Real-world result:
A well-communicated policy drives cultural alignment and fulfills a key ISO 20000 requirement for leadership involvement.

3. Roles and Responsibilities Are Unclear or Undocumented

📌 Clause: 5.3 – Organizational Roles, Responsibilities, and Authorities

What's going wrong:
Service management responsibilities — like incident handling, change authorization, and process ownership — are not clearly assigned.

Why it matters during an ISO 20000 audit:
Auditors require clear role mapping to ensure accountability. Informal delegation often leads to inconsistencies and failure to meet objectives.

How to fix it:

✓ Define roles for all core SMS activities

✓ Use a RACI matrix and document it in SMS governance records

✓ Communicate responsibilities through job descriptions and awareness sessions

Real-world result:
Clear roles reduce confusion, improve accountability, and strengthen audit confidence in SMS execution.

4. Lack of Process for Addressing Risks and Opportunities

📌 **Clause: 6.1 – Actions to Address Risks and Opportunities**

What's going wrong:
Organizations react to incidents but don't proactively assess risks or plan for opportunities to improve services.

Why it matters during an ISO 20000 audit:
Auditors look for evidence of proactive planning. Absence of risk assessment is a serious non-conformity under the 2018 version.

How to fix it:
✓ Establish a risk and opportunity assessment process
✓ Maintain a living risk register related to service delivery and continuity
✓ Review risks regularly and link mitigation plans to improvement actions

Real-world result:
Risk awareness improves service resilience, compliance readiness, and helps the SMS evolve effectively.

5. No Documented Service Management Objectives

📌 **Clause: 6.2 – Service Management Objectives and Planning**

What's going wrong:
There are no measurable objectives linked to the SMS, or they are too vague (e.g., "improve IT performance") to track effectively.

Why it matters during an ISO 20000 audit:
Objectives provide direction and evidence of continual improvement. Without them, the SMS lacks purpose and strategic value.

How to fix it:
✓ Define SMART objectives tied to business needs (e.g., reduce incident resolution time by 20%)
✓ Align objectives with the service management policy
✓ Review them during management reviews and adjust as needed

Real-world result:
Measurable goals create clarity, drive performance, and fulfill core ISO 20000 requirements.

6. Inadequate Control Over Documented Information

📌 Clause: 7.5 – Documented Information

What's going wrong:
Process documents, policies, or procedures are outdated, duplicated, or poorly controlled. Staff often refer to different versions.

Why it matters during an ISO 20000 audit:
Auditors expect proper version control, document integrity, and accessibility. Inconsistent documentation creates serious reliability issues.

How to fix it:
✓ Use a centralized system for document control (e.g., SharePoint, GRC tool)

✓ Apply versioning, approvals, and review dates to all SMS documents

✓ Restrict editing rights and log document changes

Real-world result:
Effective documentation control improves consistency, auditability, and team alignment.

7. No Structured Change Management Process

📌 **Clause: 8.2 – Change Management**

What's going wrong:
Changes to infrastructure or services are implemented without proper review, risk assessment, or rollback planning.

Why it matters during an ISO 20000 audit:
Uncontrolled changes are one of the biggest sources of service disruption. Auditors treat this as a high-risk failure.

How to fix it:

✓ Implement a structured change process for normal, standard, and emergency changes

✓ Log all changes and include impact, approval, and backout plans

✓ Conduct post-implementation reviews

Real-world result:
Structured change control reduces downtime, enhances compliance, and improves ITSM maturity.

8. Missing or Outdated Service Catalog

📌 **Clause: 8.3 – Service Delivery**

What's going wrong:
Many organizations have no formal service catalog or have one that's incomplete, outdated, or not aligned with the current SMS scope.

Why it matters during an ISO 20000 audit:
Auditors require clear visibility into the services under management. A weak catalog affects service quality and user experience.

How to fix it:
✓ Create and maintain a structured service catalog
✓ Include each service's scope, SLA, availability, owner, and support model
✓ Regularly review and update it in line with changes to services or customers

Real-world result:
An accurate service catalog supports clear communication, SLA management, and audit readiness.

9. No Evidence of Continual Improvement

📌 Clause: 10.2 – Continual Improvement

What's going wrong:
Improvements happen by chance, not design. There's no documented plan or review process to track enhancement efforts.

Why it matters during an ISO 20000 audit:
Continual improvement is central to ISO 20000. If it's not embedded in the SMS, it reflects poor governance and maturity.

How to fix it:
✓ Establish a continual improvement log with defined actions, owners, and

metrics

✓ Link improvements to risks, audits, and service feedback

✓ Review progress in management reviews

Real-world result:
A formal improvement process drives better service outcomes and shows auditors that your SMS is evolving.

10. Supplier Performance Not Monitored

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
Outsourced services are critical to operations, but organizations don't monitor supplier SLAs, review contracts, or manage risks.

Why it matters during an ISO 20000 audit:
Supplier performance affects service quality. Lack of oversight shows poor risk management and weak accountability.

How to fix it:

✓ Maintain a supplier register with SLA metrics and review timelines

✓ Conduct regular performance reviews and risk assessments

✓ Include key suppliers in change and incident processes

Real-world result:
Stronger supplier oversight improves service reliability, reduces disruptions, and builds confidence during audits.

11. No Formal Supplier Register Maintained

📌 Clause: 8.6 – Supplier Management

What's going wrong:
Organizations rely on third-party providers but don't maintain a centralized, updated register of suppliers and their roles in service delivery.

Why it matters during an ISO 20000 audit:
Auditors assess whether critical suppliers are documented and managed as part of the SMS. An absent or outdated register indicates gaps in control and risk visibility.

How to fix it:
✓ Create a detailed supplier register including contact info, services provided, contract dates, SLA terms, and risk classifications
✓ Review and update the register quarterly or after changes
✓ Use the register during audits, supplier evaluations, and incident reviews

Real-world result:
A well-maintained supplier register improves governance, supports risk analysis, and ensures traceability for external dependencies.

12. Emergency Changes Not Reviewed Post-Implementation

📌 Clause: 8.2 – Change Management

What's going wrong:
Emergency changes are implemented under pressure, but post-implementation reviews (PIRs) are rarely conducted to assess their success or risk impact.

Why it matters during an ISO 20000 audit:
Emergency changes are inherently risky. Auditors expect evidence that organizations monitor outcomes and adjust controls based on findings.

How to fix it:

✓ Define a formal PIR process specifically for emergency changes

✓ Assess what went right, what failed, and what can be improved

✓ Log PIRs and integrate findings into your change metrics

Real-world result:
Post-change analysis reduces recurring issues and enhances the maturity of your change management process.

13. Incidents Closed Without User Confirmation

📌 **Clause: 8.7 – Incident Management**

What's going wrong:
Support teams close tickets as soon as a fix is applied — without verifying resolution from the end user or confirming service restoration.

Why it matters during an ISO 20000 audit:
Auditors may flag this as a failure to meet agreed service levels and a breakdown in communication and assurance.

How to fix it:

✓ Include user confirmation as a mandatory step before incident closure (where applicable)

✓ Automate feedback or closure confirmation prompts in your ITSM tool

✓ Track and review auto-closed vs. confirmed incidents for trends

Real-world result:
User-centric incident handling improves satisfaction, closes audit gaps, and strengthens SLA credibility.

14. Service Level Agreements (SLAs) Are Missing or Incomplete

📌 **Clause: 8.3 – Service Delivery**

What's going wrong:
Some services are being delivered without formal SLAs, or the agreements lack clear performance indicators and escalation paths.

Why it matters during an ISO 20000 audit:
Without SLAs, there's no formal basis for measuring service quality or managing user expectations — both core to ITSM and audit compliance.

How to fix it:

✓ Define SLAs for every service in the catalog

✓ Include uptime, response/resolution times, and support hours

✓ Ensure SLAs are agreed upon by customers or service recipients

Real-world result:
SLAs enable transparent service delivery, strengthen user trust, and provide clear metrics for monitoring and improvement.

15. Lack of Root Cause Analysis in Problem Management

📌 **Clause: 8.8 – Problem Management**

What's going wrong:
Problems are opened and linked to incidents, but no root cause analysis (RCA) is performed to identify underlying issues.

Why it matters during an ISO 20000 audit:
RCA is central to problem management. Its absence implies reactive rather than proactive service restoration and a lost opportunity to prevent recurrence.

How to fix it:
✓ Use a structured RCA methodology (e.g., 5 Whys, Fishbone Diagram)
✓ Document causes, evidence, and contributing factors
✓ Track RCA outcomes in your problem management system

Real-world result:
Effective RCA reduces repeat incidents and downtime, boosting audit readiness and service reliability.

16. Configuration Items Not Fully Mapped or Controlled

📌 Clause: 8.9 – Configuration Management

What's going wrong:
Configuration items (CIs) are partially documented, poorly classified, or not linked to services, making impact assessments difficult.

Why it matters during an ISO 20000 audit:
Incomplete CMDBs (Configuration Management Databases) create service blind spots. Auditors need to verify traceability and control of critical components.

How to fix it:
✓ Maintain a CMDB that includes CI type, location, owner, status, and relationships

✓ Conduct periodic audits of your CMDB

✓ Integrate CI tracking with change and incident workflows

Real-world result:
Accurate CI mapping improves impact analysis, change control, and audit traceability.

17. No Formal Communication Plan for IT Services

📌 Clause: 8.5 – Relationship Management

What's going wrong:
There's no structured method to communicate service changes, outages, SLAs, or policy updates to users and stakeholders.

Why it matters during an ISO 20000 audit:
Lack of communication planning leads to stakeholder confusion, dissatisfaction, and findings related to governance gaps.

How to fix it:

✓ Develop a communication plan covering internal and external stakeholders

✓ Define frequency, channels (e.g., email, portal, meetings), and responsibilities

✓ Track communication effectiveness through feedback or surveys

Real-world result:
Structured communication improves transparency, reduces complaints, and enhances audit perception of stakeholder management.

18. Service Continuity Plans Are Unverified or Untested

📌 **Clause: 8.10 – Service Continuity Management**

What's going wrong:
Continuity plans exist but have not been tested or reviewed in the context of the current SMS or infrastructure.

Why it matters during an ISO 20000 audit:
Plans that haven't been validated offer no assurance. Auditors look for evidence that business continuity is more than just a document.

How to fix it:

✓ Test continuity plans through simulations or tabletop exercises

✓ Update based on test outcomes and operational changes

✓ Integrate continuity planning into risk assessments and change management

Real-world result:
Validated plans improve resilience, reduce downtime risk, and provide confidence during certification audits.

19. Monitoring and Measurement Data Is Not Used for Decision-Making

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

What's going wrong:
Performance data is collected but not analyzed or reviewed systematically. Decision-making relies on opinion rather than metrics.

Why it matters during an ISO 20000 audit:
Auditors expect that collected data informs continual improvement and service adjustments. Otherwise, it reflects poor operational maturity.

How to fix it:

✓ Define key metrics linked to SMS objectives

✓ Establish a review process for analyzing results

✓ Use trend reports to adjust staffing, resources, or service parameters

Real-world result:
Data-driven decision-making enhances service quality, optimizes resources, and demonstrates control during audits.

20. No Internal Audit Program for the SMS

📌 **Clause: 9.2 – Internal Audit**

What's going wrong:
The SMS is not subject to regular internal audits, or the audits lack structure, scope, or objectivity.

Why it matters during an ISO 20000 audit:
Auditors will immediately flag this as a major non-conformity. Internal audits are essential to validate compliance, drive improvement, and maintain certification.

How to fix it:

✓ Create a documented audit schedule covering all SMS processes and clauses

✓ Define scope, frequency, roles, and reporting mechanisms

✓ Train auditors or use external parties for objectivity

Real-world result:
A robust audit program enables early detection of weaknesses, continuous compliance, and a smoother path to certification.

21. Management Reviews Are Infrequent or Superficial

📌 **Clause: 9.3 – Management Review**

What's going wrong:
Management reviews are either not held regularly or lack meaningful input from service data, risk reviews, or improvement plans.

Why it matters during an ISO 20000 audit:
Auditors expect leadership to review SMS performance at planned intervals. Weak reviews reflect disengagement from governance and strategic oversight.

How to fix it:
✓ Schedule management reviews at least annually or quarterly
✓ Include performance data, audit results, objectives, risks, and improvement progress
✓ Document decisions, assigned actions, and follow-ups

Real-world result:
Structured management reviews enhance leadership alignment, decision-making, and overall SMS maturity.

22. Nonconformities Are Not Properly Recorded or Tracked

📌 **Clause: 10.1 – Nonconformity and Corrective Action**

What's going wrong:
Audit or operational findings are either not documented or not followed up with corrective action. There's no clear trail of how nonconformities are resolved.

Why it matters during an ISO 20000 audit:
Auditors require evidence of a functioning corrective action process. Without it, repeat issues are likely and continual improvement fails.

How to fix it:
✓ Create a nonconformity register or log
✓ Document each issue, root cause, corrective action, and verification steps
✓ Review open items during internal audits and management reviews

Real-world result:
Effective issue tracking builds organizational learning, reduces repeat errors, and strengthens audit readiness.

23. Continual Improvement Is Not Linked to Objectives or Metrics

📌 **Clause: 10.2 – Continual Improvement**

What's going wrong:
Improvement actions are reactive or disconnected from SMS goals. Teams implement fixes without measuring their impact or strategic relevance.

Why it matters during an ISO 20000 audit:
Improvement needs to be systematic. Auditors look for a closed loop between issues, actions, and measurable outcomes.

How to fix it:
✓ Align improvement initiatives to service management objectives and KPIs

✓ Set metrics for each improvement project

✓ Track results and adjust approach based on outcomes

Real-world result:
Linked improvements deliver measurable value and clearly demonstrate SMS effectiveness to auditors.

24. Process Descriptions Are Missing or Incomplete

📌 **Clause: 8.1 – Service Management System Planning**

What's going wrong:
Core ITSM processes like incident, change, and configuration management are not formally documented or are only partially defined.

Why it matters during an ISO 20000 audit:
Auditors need clear, documented procedures to verify process control and effectiveness. Informal processes often lead to inconsistencies.

How to fix it:

✓ Document process flows, responsibilities, inputs/outputs, and KPIs

✓ Ensure alignment with ISO 20000 clauses

✓ Review documentation during training, audits, and service reviews

Real-world result:
Complete, well-documented processes support consistent execution and pass audit scrutiny with confidence.

25. Lack of Integration Between Incident and Problem Management

📌 **Clause: 8.7 & 8.8 – Incident and Problem Management**

What's going wrong:
Incidents are logged but rarely lead to the creation of problem records. Teams miss opportunities to investigate and eliminate root causes.

Why it matters during an ISO 20000 audit:
Auditors assess how effectively you move from reactive fixes to proactive resolution. A disconnect between incidents and problems signals a maturity gap.

How to fix it:
✓ Define criteria for escalating recurring incidents to problems
✓ Automate incident-problem linkage in your ITSM tool
✓ Monitor the ratio of linked vs. standalone incidents

Real-world result:
Integrated handling reduces future incidents, speeds up resolution, and improves service reliability.

26. Change Advisory Board (CAB) Meetings Are Irregular or Ineffective

📌 **Clause: 8.2 – Change Management**

What's going wrong:
CAB meetings are canceled, inconsistent, or lack clear agendas and documentation. Change approvals are rushed or poorly informed.

Why it matters during an ISO 20000 audit:
CAB is a control mechanism for risk. Weak CAB practices can lead to poor decision-making and untracked service impacts.

How to fix it:
✓ Schedule regular CAB meetings with a formal agenda

✓ Involve stakeholders from IT, business, and security

✓ Record minutes, approvals, and follow-up actions

Real-world result:
Effective CAB meetings improve change governance, reduce service risk, and satisfy audit expectations.

27. Service Requests Are Not Distinguished from Incidents

📌 **Clause: 8.7 – Incident Management**

What's going wrong:
All tickets are treated the same — whether they're issues or standard service requests — leading to confusion and misclassification.

Why it matters during an ISO 20000 audit:
Auditors expect service request fulfillment to be handled through a distinct, controlled process separate from incident response.

How to fix it:

✓ Define separate workflows for incidents and service requests

✓ Train staff and users on categorization criteria

✓ Configure your ITSM tool to guide correct classification

Real-world result:
Improved categorization leads to better reporting, faster resolution, and cleaner audit documentation.

28. SLAs Are Not Reviewed or Updated Regularly

📌 **Clause: 8.3 – Service Delivery**

What's going wrong:
SLAs are created once and forgotten. They don't reflect changing service expectations, technologies, or customer feedback.

Why it matters during an ISO 20000 audit:
Static SLAs can result in non-conformance if services are no longer aligned with agreed performance levels.

How to fix it:

✓ Review SLAs annually or when major service changes occur

✓ Involve customers and service owners in the review process

✓ Document revisions and re-sign where applicable

Real-world result:
Up-to-date SLAs ensure relevance, maintain transparency, and show proactive service governance during audits.

29. ITSM Tooling Lacks Integration Across Processes

📌 **Clause: 8.1 – Planning and Control of SMS Processes**

What's going wrong:
Organizations use multiple tools that don't share data, leading to siloed workflows for incidents, changes, problems, and assets.

Why it matters during an ISO 20000 audit:
Disjointed systems lead to lost data, inconsistencies, and an inability to demonstrate process linkage and traceability.

How to fix it:

✓ Select ITSM tools that support integrated workflows

✓ Map data flows across processes (e.g., incident to problem to change)

✓ Train staff on using linked records effectively

Real-world result:
Tool integration enhances visibility, improves data accuracy, and simplifies evidence gathering for audits.

30. No Formal Onboarding or Training for SMS Roles

📌 **Clause: 7.2 – Competence and Awareness**

What's going wrong:
New staff assume critical SMS roles without formal onboarding or training in ISO 20000-aligned practices.

Why it matters during an ISO 20000 audit:
Auditors assess competence. A lack of training records or role-based learning undermines the effectiveness of the entire SMS.

How to fix it:

✓ Create onboarding plans for all SMS roles

✓ Deliver periodic training on ITSM processes, tools, and ISO 20000 principles

✓ Maintain training records and conduct annual refreshers

Real-world result:
Trained staff execute processes more effectively and confidently explain their roles during audits.

31. Lack of Defined Criteria for Prioritizing Incidents

📌 **Clause: 8.7 – Incident Management**

What's going wrong:
Incidents are logged but prioritized inconsistently. Support teams use personal judgment rather than standardized urgency/impact matrices.

Why it matters during an ISO 20000 audit:
Auditors expect defined criteria for consistent and justifiable prioritization. Unstructured prioritization delays resolution and compromises service targets.

How to fix it:

✓ Implement an impact/urgency matrix for all incoming incidents

✓ Train service desk staff on its application

✓ Audit ticket data periodically to ensure compliance with the matrix

Real-world result:
Standardized prioritization ensures timely resolution, supports SLA compliance, and demonstrates operational maturity to auditors.

32. Inadequate Review of Risks Affecting Third-Party Services

📌 **Clause: 6.1 & 8.6 – Risk Management and Supplier Management**

What's going wrong:
Risk assessments overlook services or infrastructure managed by suppliers, exposing the organization to blind spots.

Why it matters during an ISO 20000 audit:
Auditors expect supplier risks to be evaluated as part of the SMS. Failure to address them weakens resilience and service assurance.

How to fix it:

✓ Include third-party services in your IT risk assessments

✓ Engage suppliers in risk identification and mitigation discussions

✓ Maintain documentation in your risk register

Real-world result:
Stronger third-party risk visibility improves service reliability and shows proactive governance.

33. No Evidence of Customer Satisfaction Monitoring

📌 **Clause: 8.5 – Relationship Management**

What's going wrong:
Organizations rely on informal conversations or anecdotal feedback instead of structured satisfaction surveys or metrics.

Why it matters during an ISO 20000 audit:
Auditors expect measurable evidence of user and customer satisfaction. Lack of data may lead to non-conformance under relationship management.

How to fix it:

✓ Conduct regular satisfaction surveys or feedback sessions

✓ Define metrics such as Net Promoter Score (NPS), response rate, or satisfaction trends

✓ Link feedback to improvement actions

Real-world result:
Measuring satisfaction helps organizations align services with expectations and strengthens user relationships.

34. No Testing of Incident Escalation Procedures

📌 Clause: 8.7 – Incident Management

What's going wrong:
Escalation procedures are documented but untested. Teams don't know who to escalate to during high-priority or unresolved incidents.

Why it matters during an ISO 20000 audit:
Auditors look for assurance that critical incident handling is effective. Without testing, you can't prove the procedure works.

How to fix it:
✓ Simulate P1/P2 incident scenarios to validate escalation workflows
✓ Review escalation paths with all relevant teams
✓ Document lessons learned and update workflows

Real-world result:
Validated escalation procedures reduce downtime, improve user trust, and boost audit credibility.

35. IT Asset Inventory Is Incomplete or Unlinked to Services

📌 Clause: 8.9 – Configuration Management

What's going wrong:
Asset data is scattered or only partially maintained. CIs are not linked to services, making troubleshooting and impact analysis harder.

Why it matters during an ISO 20000 audit:
Auditors require traceability of CIs to services. A disconnected asset database hinders problem resolution and control effectiveness.

How to fix it:

✓ Maintain a centralized CMDB with all relevant configuration items

✓ Map assets to services, users, and support teams

✓ Conduct regular audits to reconcile data accuracy

Real-world result:

A complete, service-linked asset inventory enhances efficiency, speeds up change/incident management, and satisfies audit criteria.

36. Service Continuity Risks Are Not Reviewed Periodically

📌 **Clause: 8.10 – Service Continuity Management**

What's going wrong:

Continuity-related risks are identified once and never revisited, even after major changes in business or infrastructure.

Why it matters during an ISO 20000 audit:

Risk is dynamic. Auditors expect ongoing continuity assessments to reflect current operations and threats.

How to fix it:

✓ Review continuity risks at least annually or after major changes

✓ Link risk reassessment to your change management and supplier reviews

✓ Update continuity plans based on reassessment findings

Real-world result:

Ongoing risk review strengthens resilience and ensures your SMS remains responsive to emerging threats.

37. Lack of Traceability Between SLAs and Underpinning Contracts (UCs)

📌 **Clause: 8.3 – Service Delivery & 8.6 – Supplier Management**

What's going wrong:
SLAs define expectations for users, but the organization fails to ensure that internal teams or vendors are contractually aligned to deliver them.

Why it matters during an ISO 20000 audit:
Without underpinning contracts or OLAs, SLA breaches become untraceable — raising accountability concerns.

How to fix it:

✓ Map every SLA to a supporting UC or OLA

✓ Align supplier performance metrics with SLA targets

✓ Review and update contracts when services or SLAs change

Real-world result:
Stronger SLA alignment across internal and external contributors improves service reliability and accountability.

38. Service Reports Are Infrequent or Incomplete

📌 **Clause: 9.1 – Monitoring and Evaluation**

What's going wrong:
Service reporting is irregular or lacks relevant KPIs. Reports may exclude SLA compliance, service interruptions, or improvement tracking.

Why it matters during an ISO 20000 audit:
Auditors rely on reports to assess SMS performance. Weak reporting suggests lack of monitoring and governance oversight.

How to fix it:

✓ Establish a regular reporting cycle (monthly or quarterly)

✓ Include SLA trends, incident volumes, change success rates, and improvement actions

✓ Distribute reports to leadership and service owners

Real-world result:

Timely, complete reporting enhances visibility, decision-making, and audit transparency.

39. Customer-Facing Services Not Linked to SMS Processes

📌 **Clause: 4.3 & 8.1 – SMS Scope and Planning**

What's going wrong:

Some customer-facing services are supported but not formally integrated into SMS processes like incident, change, or SLA tracking.

Why it matters during an ISO 20000 audit:

All in-scope services must be under control. Gaps between delivered services and SMS coverage are major audit red flags.

How to fix it:

✓ Reconcile your actual service portfolio with the SMS scope and service catalog

✓ Ensure each service is tied to processes for delivery, support, and measurement

✓ Update scope documentation and team responsibilities accordingly

Real-world result:

Bringing all services into SMS control closes compliance gaps and improves user experience.

40. No Review of Policy Effectiveness or Relevance

📌 **Clause: 5.2 – Service Management Policy**

What's going wrong:
The policy is published but never reviewed to determine whether it reflects current objectives, risks, or operational needs.

Why it matters during an ISO 20000 audit:
Policies must evolve with the business. Auditors will note misalignment between static policies and current ITSM practices.

How to fix it:
✓ Schedule annual policy reviews as part of the management review cycle
✓ Evaluate alignment with goals, risks, and customer expectations
✓ Update version history and communicate changes across the organization

Real-world result:
A dynamic, reviewed policy keeps your SMS relevant, compliant, and strategically aligned.

41. No Documented Criteria for Accepting Residual Risks

📌 **Clause: 6.1 – Actions to Address Risks and Opportunities**

What's going wrong:
Residual risks are marked as "accepted" without formal documentation or justification. Acceptance is often based on verbal agreements or assumptions.

Why it matters during an ISO 20000 audit:
Auditors expect risk decisions to be documented, traceable, and aligned with risk appetite. Lack of clarity raises governance concerns.

How to fix it:

✓ Define criteria for acceptable residual risk levels

✓ Require formal approval from authorized roles (e.g., Risk Owner, Service Owner)

✓ Document the rationale for acceptance in the risk register

Real-world result:
Clear risk acceptance processes improve accountability and build trust with stakeholders and auditors.

42. Roles Are Not Reviewed After Organizational Changes

📌 **Clause: 5.3 – Organizational Roles, Responsibilities and Authorities**

What's going wrong:
Changes in team structure or staffing occur, but SMS roles and process ownership are not updated accordingly.

Why it matters during an ISO 20000 audit:
Undefined or outdated roles result in misalignment and lack of accountability — a common audit finding.

How to fix it:

✓ Revalidate SMS roles after reorganizations, promotions, or staff turnover

✓ Update RACI matrices and access controls

✓ Communicate changes through onboarding or refresher training

Real-world result:
Updated roles maintain process ownership and ensure continuity in SMS accountability.

43. Improvement Actions Are Not Tracked to Completion

📌 **Clause: 10.2 – Continual Improvement**

What's going wrong:
Improvement initiatives are initiated but forgotten or remain incomplete. There's no mechanism to track, follow up, or validate effectiveness.

Why it matters during an ISO 20000 audit:
Continual improvement must be demonstrable. Unfinished actions reflect poorly on governance and planning.

How to fix it:
✓ Maintain a central log of all improvement actions with owners and deadlines
✓ Review progress in management reviews or operational meetings
✓ Validate and document results before closing actions

Real-world result:
Tracked improvements boost audit confidence and drive service evolution.

44. No Defined Metrics for Key ITSM Processes

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

What's going wrong:
Processes like incident, change, or configuration management operate without defined KPIs or success metrics.

Why it matters during an ISO 20000 audit:
Auditors expect evidence of process performance. Without metrics, evaluation becomes subjective and incomplete.

How to fix it:
✓ Define KPIs for each SMS process (e.g., mean time to resolution, change success rate)
✓ Set thresholds and track performance trends
✓ Use metrics to inform improvements and decisions

Real-world result:
Meaningful metrics enable proactive management and clear audit evidence of control.

45. Service Restoration Targets Are Not Documented

📌 **Clause: 8.10 – Service Continuity Management**

What's going wrong:
The organization lacks defined Recovery Time Objectives (RTOs) or restoration priorities for critical services.

Why it matters during an ISO 20000 audit:
Without restoration targets, continuity planning lacks direction, and post-disruption actions may be misaligned.

How to fix it:
✓ Define RTOs and Recovery Point Objectives (RPOs) for each critical service

✓ Include these in continuity and SLA documentation

✓ Validate targets through business impact analysis (BIA) and testing

Real-world result:
Clear restoration targets strengthen continuity, stakeholder trust, and audit readiness.

46. Supplier Risks Are Not Integrated into Service Planning

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
Supplier-related risks (e.g., contract expiration, performance gaps) are not addressed during service design or reviews.

Why it matters during an ISO 20000 audit:
Auditors expect integrated risk management across the SMS. Overlooking supplier risks leaves critical dependencies unmanaged.

How to fix it:

✓ Include supplier risk assessments in service reviews

✓ Maintain supplier risk entries in the SMS risk register

✓ Link supplier performance and risk to SLA outcomes

Real-world result:
Integrated supplier risk controls improve service continuity and reduce audit exposure.

47. Configuration Management Policy Is Missing or Unenforced

📌 **Clause: 8.9 – Configuration Management**

What's going wrong:
There's no formal policy defining how configuration items (CIs) are identified, maintained, or updated.

Why it matters during an ISO 20000 audit:
A missing or weak policy leads to uncontrolled assets and broken CI traceability — common sources of audit non-conformities.

How to fix it:

✓ Develop a CI policy covering scope, naming conventions, lifecycle, and relationships

✓ Communicate the policy to IT operations and change teams

✓ Audit CI data for compliance with the policy

Real-world result:
A solid CM policy boosts visibility, reduces change errors, and satisfies configuration-related audit requirements.

48. Unclear Ownership for Service Performance Monitoring

📌 **Clause: 9.1 – Monitoring and Evaluation**

What's going wrong:
Service metrics are gathered, but it's unclear who is accountable for monitoring, interpreting, and acting on them.

Why it matters during an ISO 20000 audit:
Auditors assess whether the SMS has active oversight. Metrics without ownership reduce control and improvement value.

How to fix it:

✓ Assign metric owners in process documentation or job roles

✓ Define escalation paths if targets are missed

✓ Review ownership during management and performance meetings

Real-world result:
Accountability drives responsiveness, transparency, and performance in the SMS.

49. No Clear Definition of Emergency Changes

📌 **Clause: 8.2 – Change Management**

What's going wrong:
"Emergency change" is used broadly and inconsistently, sometimes bypassing approvals or reviews.

Why it matters during an ISO 20000 audit:
Auditors require clear classification to ensure process integrity and reduce misuse of emergency channels.

How to fix it:

✓ Define what qualifies as an emergency change (e.g., critical outage restoration)

✓ Document criteria, approval steps, and post-review requirements

✓ Train staff to distinguish emergency vs. normal changes

Real-world result:
Better change control reduces operational risk and earns auditor confidence in your governance.

50. Limited Involvement of End Users in Feedback and Design

📌 **Clause: 8.5 – Relationship Management**

What's going wrong:
End users are rarely engaged in evaluating services, providing feedback, or co-developing improvement ideas.

Why it matters during an ISO 20000 audit:
Auditors assess user involvement as part of relationship management. Lack of feedback loops weakens service quality assurance.

How to fix it:
✓ Involve users in service reviews, design workshops, and feedback surveys
✓ Track themes and insights from user input
✓ Use feedback to prioritize improvements

Real-world result:
User-inclusive SMS development improves relevance, satisfaction, and transparency in the audit process.

51. Problem Records Lack Closure Criteria or Verification

📌 **Clause: 8.8 – Problem Management**

What's going wrong:
Problem tickets are marked as closed without verifying that corrective actions were implemented or that incidents have ceased.

Why it matters during an ISO 20000 audit:
Auditors expect structured closure with evidence of effectiveness. Premature closure may hide unresolved root causes.

How to fix it:

✓ Define closure criteria for problems (e.g., verified solution, monitored period without recurrence)

✓ Require documented verification before closure

✓ Review problem logs during internal audits

Real-world result:
Stronger problem closure improves service reliability and demonstrates proactive resolution to auditors.

52. Service Impact Is Not Considered During Change Evaluation

📌 **Clause: 8.2 – Change Management**

What's going wrong:
Changes are approved based on technical feasibility without analyzing the potential business or service-level impact.

Why it matters during an ISO 20000 audit:
Auditors expect service-aware change evaluation. Ignoring impact leads to SLA breaches, downtime, or reputational damage.

How to fix it:

✓ Add service impact as a required evaluation field for all changes

✓ Involve service owners in high-risk change approvals

✓ Use pre-implementation risk ratings to guide planning

Real-world result:
Service-aware change processes reduce disruption and satisfy auditors with holistic planning.

53. Internal Communication of Policies and Processes Is Weak

📌 **Clause: 7.3 – Awareness**

What's going wrong:
Staff are unaware of SMS policies, procedures, or their roles within them. Communication is informal and inconsistent.

Why it matters during an ISO 20000 audit:
Auditors assess awareness levels. If staff can't articulate the SMS or their part in it, it reflects poor engagement and training.

How to fix it:

✓ Conduct regular awareness sessions or policy refreshers

✓ Include SMS materials in onboarding programs

✓ Test awareness through spot checks or surveys

Real-world result:
Improved internal communication strengthens ownership, execution, and audit performance.

54. Monitoring Tools Are Not Calibrated or Reviewed

📌 **Clause: 9.1 – Monitoring and Measurement**

What's going wrong:
Monitoring systems may miss events or generate false positives due to outdated configurations, thresholds, or integrations.

Why it matters during an ISO 20000 audit:
Auditors evaluate the reliability of monitoring data. Poor calibration undermines incident detection and SLA assurance.

How to fix it:

✓ Review monitoring rules and thresholds quarterly

✓ Align metrics with updated SLAs and services

✓ Log and analyze missed alerts to adjust configurations

Real-world result:
Reliable monitoring enables faster response times and builds confidence in ITSM oversight.

55. Backup and Recovery Procedures Are Not Tested

📌 **Clause: 8.10 – Service Continuity Management**

What's going wrong:
Backups are scheduled, but recovery has not been tested — leaving uncertainty about restoration time and data integrity.

Why it matters during an ISO 20000 audit:
Untested procedures are a major risk. Auditors expect evidence of successful restoration drills.

How to fix it:

✓ Test backup restorations periodically (e.g., quarterly)

✓ Simulate failure scenarios for critical systems

✓ Document outcomes and lessons learned

Real-world result:
Tested backups improve business resilience and assure auditors of continuity capability.

56. No Clear Link Between Services and Their Supporting Infrastructure

📌 **Clause: 8.9 – Configuration Management**

What's going wrong:
Services are defined, but not mapped to the infrastructure or assets that support them, limiting impact assessments and troubleshooting.

Why it matters during an ISO 20000 audit:
Auditors assess whether dependencies are documented and traceable. Missing links impair change planning and risk response.

How to fix it:
✓ Map all services to their configuration items (CIs)
✓ Use your CMDB to document relationships
✓ Update mappings after changes to services or infrastructure

Real-world result:
Better visibility into dependencies enables faster recovery and stronger service governance.

57. Incidents and Problems Are Not Categorized Consistently

📌 **Clause: 8.7 & 8.8 – Incident and Problem Management**

What's going wrong:
Classification rules vary between teams. Similar issues are logged under different categories, distorting reports and trends.

Why it matters during an ISO 20000 audit:
Auditors review data consistency. Poor categorization weakens trend analysis and process control.

How to fix it:

✓ Define standard classification rules and categories

✓ Train service desk and support teams on their application

✓ Audit ticket logs for consistency and correct where needed

Real-world result:
Clean, consistent data supports smarter decisions and strong audit evidence.

58. No KPI Review Cycle Defined

📌 **Clause: 9.1 – Monitoring and Evaluation**

What's going wrong:
KPIs are tracked but not reviewed formally or regularly, so performance trends and root causes go unnoticed.

Why it matters during an ISO 20000 audit:
Measurement must lead to action. If KPIs are passive, they lose their compliance and operational value.

How to fix it:

✓ Define a monthly or quarterly KPI review cadence

✓ Assign roles to lead reviews and recommend actions

✓ Document findings and action plans

Real-world result:
Consistent review ensures metrics are used for governance, improvement, and audit assurance.

59. Review of Contracts and SLAs Is Not Scheduled

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
Service-level and vendor contracts are left untouched for years, even as services evolve or performance declines.

Why it matters during an ISO 20000 audit:
Auditors expect SLAs and UCs to reflect current service needs and risks. Outdated documents create misalignment and exposure.

How to fix it:

✓ Schedule annual SLA and UC reviews

✓ Involve legal, service owners, and vendors in the process

✓ Document updates and performance metrics

Real-world result:
Updated agreements maintain relevance, minimize disputes, and reinforce trust in supplier relationships.

60. The SMS Does Not Include All In-Scope Locations or Departments

📌 **Clause: 4.3 – Scope of the SMS**

What's going wrong:
The defined scope lists services but omits the physical locations or departments responsible for delivery or support.

Why it matters during an ISO 20000 audit:
Auditors must confirm that all involved entities fall under the SMS. Gaps in scope lead to non-conformities.

How to fix it:

✓ Revisit the SMS scope and verify it includes all relevant sites, teams, and technologies

✓ Align with service maps, support models, and operational structures

✓ Communicate scope updates organization-wide

Real-world result:
A complete scope ensures that your SMS is comprehensive, compliant, and audit-ready.

61. Capacity Planning Is Reactive, Not Strategic

📌 **Clause: 8.4 – Capacity and Performance Management**

What's going wrong:
Organizations address capacity only when performance issues arise. There's no forecasting or planning based on service growth or business trends.

Why it matters during an ISO 20000 audit:
Auditors expect proactive management of capacity to meet service expectations. Reactive handling leads to service degradation and audit flags.

How to fix it:

✓ Implement regular capacity reviews based on service demand

✓ Use trend data to forecast resource needs (e.g., storage, bandwidth, licenses)

✓ Link capacity planning to change and service design processes

Real-world result:
Proactive planning minimizes performance issues and ensures scalable, reliable service delivery.

62. No Review of Service Level Targets Against Business Needs

📌 **Clause: 8.3 – Service Delivery**

What's going wrong:
SLAs are created once and not revisited, even when user expectations or business processes change.

Why it matters during an ISO 20000 audit:
Misaligned SLAs fail to reflect service priorities. Auditors may question your SMS's responsiveness to evolving needs.

How to fix it:
✓ Review SLAs with business stakeholders annually or after major changes
✓ Adjust targets and metrics as needed to reflect priorities
✓ Document revisions and track approvals

Real-world result:
Updated SLAs drive business alignment and prevent service dissatisfaction.

63. Changes Are Not Linked to Configuration Items (CIs)

📌 **Clause: 8.2 & 8.9 – Change and Configuration Management**

What's going wrong:
Changes are processed without identifying the affected CIs, making impact analysis and troubleshooting difficult.

Why it matters during an ISO 20000 audit:
Auditors expect traceability. Linking changes to CIs is essential for risk management and post-implementation review.

How to fix it:

✓ Require CI association during change logging

✓ Use the CMDB to auto-populate affected items

✓ Review CI links during CAB discussions

Real-world result:
Greater traceability reduces outage risks and supports accurate impact analysis.

64. Risk Assessments Are Not Updated After Incidents or Changes

📌 **Clause: 6.1 – Risk and Opportunity Management**

What's going wrong:
Even after major disruptions or infrastructure changes, the risk register remains unchanged — missing emerging threats or shifts in impact.

Why it matters during an ISO 20000 audit:
Auditors assess whether your SMS adapts to operational events. Stale risk assessments reflect poor responsiveness.

How to fix it:

✓ Update risks after major incidents, changes, or supplier issues

✓ Review likelihood and impact scores with new data

✓ Use a change-triggered risk review checklist

Real-world result:
Up-to-date risk analysis ensures your SMS evolves with business and operational realities.

65. No Records of Emergency Change Reviews

📌 **Clause: 8.2 – Change Management**

What's going wrong:
Emergency changes are applied quickly, but not reviewed afterward — missing potential risks, failures, or process improvements.

Why it matters during an ISO 20000 audit:
Post-implementation reviews are a control requirement. Without them, change management appears unmanaged.

How to fix it:
✓ Schedule mandatory post-review for all emergency changes
✓ Include risk analysis, success evaluation, and rollback testing
✓ Record outcomes and feed into improvement cycles

Real-world result:
Post-reviews reduce risk recurrence and improve emergency handling credibility.

66. No Defined Escalation Path in Incident or Request Management

📌 **Clause: 8.7 – Incident Management**

What's going wrong:
When resolution stalls, support teams are unclear on whom to escalate to — leading to delays and poor service recovery.

Why it matters during an ISO 20000 audit:
Auditors expect defined, documented escalation processes to maintain SLA commitments.

How to fix it:

✓ Define tiered escalation paths by priority/severity

✓ Include them in SOPs and ticketing tools

✓ Train staff to escalate early and appropriately

Real-world result:
Effective escalation accelerates resolution and helps meet SLA targets consistently.

67. No Integration Between IT Service Continuity and Incident Management

📌 **Clause: 8.7 & 8.10 – Incident and Continuity Management**

What's going wrong:
Critical incidents occur, but continuity procedures are not invoked, tested, or aligned with incident handling processes.

Why it matters during an ISO 20000 audit:
Continuity and incident response must work together to protect critical services. Lack of integration reduces responsiveness.

How to fix it:

✓ Link continuity plans to high-severity incident types

✓ Define triggers for plan activation

✓ Include continuity scenarios in incident response testing

Real-world result:
Stronger integration improves recovery and ensures coordinated response during disruptions.

68. No Trend Analysis of Change-Related Incidents

📌 **Clause: 8.2 & 8.7 – Change and Incident Management**

What's going wrong:
Incidents caused by failed or misconfigured changes are not tracked or analyzed as a group, so recurring patterns go unnoticed.

Why it matters during an ISO 20000 audit:
Auditors assess whether incident data is used to improve change success rates. Missed trends reduce control effectiveness.

How to fix it:

✓ Tag incidents linked to failed or impactful changes

✓ Analyze patterns monthly and report to CAB

✓ Use insights to refine change evaluation criteria

Real-world result:
Trend analysis reduces change-related outages and supports continual process refinement.

69. Customer-Facing SLAs Are Not Linked to Internal OLAs

📌 **Clause: 8.3 & 8.6 – Service Delivery and Supplier Management**

What's going wrong:
End-user SLA targets (e.g., 4-hour resolution) are not supported by internal team or vendor agreements, making delivery unrealistic.

Why it matters during an ISO 20000 audit:
Auditors look for consistency between external commitments and internal capabilities. Disconnected SLAs risk non-delivery.

How to fix it:

✓ Define OLAs and Underpinning Contracts that directly support SLA terms

✓ Monitor performance alignment across the layers

✓ Review internal targets when SLAs change

Real-world result:
Linked agreements build delivery confidence and clarify expectations across the service chain.

70. Lack of Awareness of Service Dependencies During Planning

📌 **Clause: 8.1 – Service Planning**

What's going wrong:
When designing or modifying services, teams overlook technical or human dependencies (e.g., licensing, support staff availability).

Why it matters during an ISO 20000 audit:
Planning without dependency awareness leads to service failure risks and weakens the SMS foundation.

How to fix it:

✓ Conduct a dependency analysis during service design and change planning

✓ Include upstream/downstream systems, roles, and suppliers

✓ Review dependencies during risk assessments and service reviews

Real-world result:
Robust planning improves service stability, mitigates rollout risks, and earns audit confidence.

71. No Service Quality Objectives for Individual Teams or Processes

📌 **Clause: 6.2 – Service Management Objectives**

What's going wrong:
The organization sets top-level objectives but doesn't break them down into department- or process-level targets.

Why it matters during an ISO 20000 audit:
Auditors want to see how SMS objectives cascade into operational execution. Without alignment, ownership and progress tracking suffer.

How to fix it:
✓ Translate SMS goals into measurable objectives for IT teams and process owners
✓ Align KPIs with individual and departmental roles
✓ Review progress quarterly in service or ops reviews

Real-world result:
Granular objectives promote accountability and create stronger links between strategy and day-to-day service delivery.

72. No Clear Lifecycle for Process Improvement Initiatives

📌 **Clause: 10.2 – Continual Improvement**

What's going wrong:
Improvements are initiated but lack follow-through, ownership, or review — leading to incomplete execution or repetition of issues.

Why it matters during an ISO 20000 audit:
Auditors assess the effectiveness of continual improvement. Incomplete initiatives reflect poor governance.

How to fix it:

✓ Define an improvement lifecycle: identify → plan → implement → verify → close

✓ Assign owners, due dates, and success criteria

✓ Document and review completed actions during management review

Real-world result:
A structured lifecycle builds discipline, accountability, and auditability into your improvement efforts.

73. Availability Management Is Not Addressed or Defined

📌 **Clause: 8.4 – Availability Management**

What's going wrong:
There is no formal strategy for maintaining or improving availability of key services — only reactive incident resolution.

Why it matters during an ISO 20000 audit:
Availability is a core service value. Lack of planning reduces your ability to meet business expectations or sustain SLAs.

How to fix it:

✓ Define service availability goals and critical uptime periods

✓ Monitor availability trends across services

✓ Investigate and correct recurring unavailability issues

Real-world result:
Availability management improves uptime, customer satisfaction, and resilience — while reducing SLA penalties.

74. User Training on Request and Incident Logging Is Not Provided

📌 **Clause: 8.5 – Relationship Management**

What's going wrong:
End users don't know how to raise requests or report incidents correctly, leading to delays, misroutes, or incomplete tickets.

Why it matters during an ISO 20000 audit:
Service quality depends on user interaction. Auditors expect proactive communication and training on request channels.

How to fix it:

✓ Conduct onboarding and refresher training for end users

✓ Provide service desk contact methods and response timelines

✓ Include guides in your self-service portal or intranet

Real-world result:
Educated users improve ticket quality, reduce response time, and reduce first-line support strain.

75. Roles Are Not Mapped to Competence Requirements

📌 **Clause: 7.2 – Competence**

What's going wrong:
SMS-related roles are assigned, but there is no matching of job responsibilities to required skills, certifications, or knowledge.

Why it matters during an ISO 20000 audit:
Auditors want assurance that personnel are qualified to perform their SMS duties — not just assigned by title.

How to fix it:

✓ Define competence profiles for SMS roles (e.g., Change Manager, CAB Chair)

✓ Conduct gap analysis and create training plans

✓ Maintain updated training records and certifications

Real-world result:
Role-based competence ensures qualified service delivery and builds trust with stakeholders and auditors.

76. No Communication of Supplier-Related Risks to Stakeholders

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
Supplier issues like poor delivery or compliance risks are known internally but not escalated to service owners or customers.

Why it matters during an ISO 20000 audit:
Auditors expect transparency and risk awareness across the SMS. Suppressed supplier risks lead to audit and operational failures.

How to fix it:

✓ Include supplier performance and risks in regular service reviews

✓ Define escalation paths for supplier risk events

✓ Update risk registers and SLA discussions accordingly

Real-world result:
Transparent supplier risk management improves accountability and allows proactive customer communication.

77. Service Reporting Is Not Role-Specific or Actionable

📌 **Clause: 9.1 – Monitoring and Evaluation**

What's going wrong:
All stakeholders receive the same generic report, making it unclear what actions are needed or who owns performance issues.

Why it matters during an ISO 20000 audit:
Auditors look for effective communication that enables decisions. Poor targeting wastes effort and undermines engagement.

How to fix it:

✓ Customize reports for executives, service owners, and technical teams

✓ Include recommendations and assigned action items

✓ Review outcomes at appropriate governance forums

Real-world result:
Targeted reporting drives engagement, accountability, and meaningful service improvements.

78. Process Interactions Are Not Documented or Understood

📌 **Clause: 8.1 – SMS Planning**

What's going wrong:
Each process (e.g., change, incident, asset) is managed in isolation with no clarity on how they intersect or depend on one another.

Why it matters during an ISO 20000 audit:
The SMS is a system. Auditors expect visibility into process integration to verify control across workflows.

How to fix it:

✓ Create a process interaction diagram or matrix

✓ Define data, role, and trigger relationships between processes

✓ Train teams to understand and operate across boundaries

Real-world result:
Integrated processes reduce silos, improve response time, and support end-to-end service performance.

79. SLA Failures Are Not Investigated or Followed Up

📌 **Clause: 8.3 – Service Delivery**

What's going wrong:
When SLA breaches occur, there's no documented review or follow-up to identify the cause and prevent recurrence.

Why it matters during an ISO 20000 audit:
Auditors want to see active service governance. Ignoring SLA failures signals weak accountability and continual improvement.

How to fix it:

✓ Review each breach to determine cause and responsible area

✓ Log corrective actions and assign ownership

✓ Communicate outcomes to stakeholders

Real-world result:
Systematic follow-up improves SLA performance and closes the loop on service quality assurance.

80. Customer Complaints Are Not Logged or Analyzed Systematically

📌 **Clause: 8.5 – Relationship Management**

What's going wrong:
Complaints are handled informally or by individual teams, with no central logging, analysis, or review.

Why it matters during an ISO 20000 audit:
Auditors expect structured complaint handling as part of service relationship governance.

How to fix it:

✓ Log all complaints in a central system or register

✓ Categorize by type, service, or root cause

✓ Analyze trends and link to improvement or risk actions

Real-world result:
Complaint analysis leads to service design insights and helps demonstrate customer-centric management.

81. Process Documentation Is Not Version Controlled

📌 **Clause: 7.5 – Documented Information**

What's going wrong:
Policies, procedures, and templates exist but lack formal version control — making it unclear which version is current or approved.

Why it matters during an ISO 20000 audit:
Auditors require evidence of controlled documentation to ensure consistency and prevent outdated practices.

How to fix it:

✓ Use a version control system or naming convention (e.g., v2.1, with date and approver)

✓ Track revisions and review cycles

✓ Ensure only approved documents are accessible to staff

Real-world result:
Controlled documents ensure consistent execution and reliable audit evidence.

82. Risk Owners Are Not Assigned to Key Risks

📌 **Clause: 6.1 – Actions to Address Risks and Opportunities**

What's going wrong:
Risks are logged in a register, but no one is accountable for tracking mitigation or escalation.

Why it matters during an ISO 20000 audit:
Auditors expect each risk to have a clear owner responsible for follow-through. Lack of ownership equals unmanaged risk.

How to fix it:

✓ Assign a named owner for each risk entry

✓ Define roles in the risk management procedure

✓ Review ownership status during audits and risk meetings

Real-world result:
Named ownership ensures follow-up, action, and a strong risk governance posture.

83. Configuration Items Are Not Audited for Accuracy

📌 **Clause: 8.9 – Configuration Management**

What's going wrong:
The CMDB contains outdated, duplicate, or incorrect configuration data — affecting change and incident management accuracy.

Why it matters during an ISO 20000 audit:
Auditors require reliable configuration data for traceability and impact analysis.

How to fix it:
✓ Schedule regular audits and reconciliation of CIs
✓ Use discovery tools or cross-check against asset inventories
✓ Update or remove stale records promptly

Real-world result:
Accurate CI data supports better change control, faster issue resolution, and higher audit confidence.

84. KPIs Are Not Aligned With Strategic Objectives

📌 **Clause: 6.2 & 9.1 – Objectives and Monitoring**

What's going wrong:
Service metrics are reported, but they don't tie back to SMS goals or customer value — making them irrelevant for strategic decisions.

Why it matters during an ISO 20000 audit:
Auditors look for KPIs that track real service outcomes, not vanity metrics.

How to fix it:

✓ Align KPIs with policy objectives and business outcomes (e.g., customer satisfaction, response time, availability)

✓ Review KPIs annually for relevance

✓ Remove unused or redundant metrics

Real-world result:
Relevant KPIs make reporting more valuable and improvements more focused.

85. No Documentation of Lessons Learned from Major Incidents

📌 **Clause: 8.7 – Incident Management**

What's going wrong:
Major incidents are resolved, but there's no formal review to capture lessons learned, contributing factors, or preventive actions.

Why it matters during an ISO 20000 audit:
Auditors expect continual improvement. Skipping post-incident analysis shows missed opportunities.

How to fix it:

✓ Conduct structured reviews after high-impact incidents

✓ Document root causes, mitigations, and improvement actions

✓ Assign owners and track implementation

Real-world result:
Lessons learned improve process maturity and resilience against repeat issues.

86. Risk Appetite or Tolerance Levels Are Not Defined

📌 **Clause: 5.1 & 6.1 – Leadership and Risk Planning**

What's going wrong:
There's no clear threshold for what level of risk is acceptable — causing inconsistent decision-making and unclear escalation triggers.

Why it matters during an ISO 20000 audit:
Auditors expect defined risk thresholds to guide treatment and prioritization.

How to fix it:
✓ Define risk tolerance levels per category (e.g., financial, operational, reputational)
✓ Document thresholds in the risk management policy
✓ Use them to trigger escalations and decisions

Real-world result:
A defined risk appetite improves decision-making and creates audit-ready clarity.

87. No Review or Testing of Onboarding and Offboarding Procedures

📌 **Clause: 7.2 – Competence and Awareness**

What's going wrong:
New hires and departing employees are not consistently provisioned or deprovisioned — creating gaps in access control and training.

Why it matters during an ISO 20000 audit:
Auditors examine role readiness and system access as part of control effectiveness.

How to fix it:

✓ Define onboarding/offboarding steps with process ownership

✓ Automate checklists and approvals

✓ Periodically test the process and document results

Real-world result:
Secure, standardized onboarding ensures faster role readiness and minimizes access risk.

88. No Integration of Incident and Capacity Data

📌 **Clause: 8.4 & 8.7 – Capacity and Incident Management**

What's going wrong:
Capacity constraints cause repeated incidents, but the data is not linked, so root causes go undetected.

Why it matters during an ISO 20000 audit:
Auditors expect that service data informs decisions and improvements.

How to fix it:

✓ Cross-analyze capacity alerts and incident trends

✓ Escalate to problem management if recurring

✓ Feed insights into planning and change processes

Real-world result:
Integrated analysis improves reliability and allows smarter capacity decisions.

89. Communication of Changes to End Users Is Inconsistent

📌 Clause: 8.2 & 8.5 – Change Management and Relationship Management

What's going wrong:
Users are often surprised by changes or updates, leading to confusion, complaints, or avoidable support tickets.

Why it matters during an ISO 20000 audit:
Auditors assess change communication as a key part of service reliability and stakeholder trust.

How to fix it:
✓ Define communication protocols based on change category and impact
✓ Notify users in advance with clear messaging and timelines
✓ Monitor communication effectiveness through feedback

Real-world result:
Clear communication improves user satisfaction and smooths change rollouts.

90. Service Reports Do Not Include Historical Trends

📌 Clause: 9.1 – Monitoring and Evaluation

What's going wrong:
Reports only show monthly performance, lacking trend analysis that identifies patterns, improvements, or degradation over time.

Why it matters during an ISO 20000 audit:
Auditors expect trend data to assess continual improvement and risk detection.

How to fix it:

✓ Include 3–6 months of KPI history in service reports

✓ Highlight trend lines, anomalies, and root cause insights

✓ Review in service meetings and management reviews

Real-world result:
Historical trends support long-term planning and demonstrate service evolution to auditors and stakeholders.

91. Service Continuity Plans Are Not Reviewed After Major Changes

📌 **Clause: 8.10 – Service Continuity Management**

What's going wrong:
Continuity plans remain static despite major organizational or infrastructure changes — making them outdated and ineffective in a real crisis.

Why it matters during an ISO 20000 audit:
Auditors expect continuity plans to reflect current systems, people, and dependencies. Outdated plans = audit exposure.

How to fix it:

✓ Trigger continuity plan reviews after structural, service, or supplier changes

✓ Involve relevant stakeholders in the update process

✓ Validate changes through tabletop or real scenario testing

Real-world result:
Up-to-date continuity planning enhances resilience and reassures auditors of true preparedness.

92. Lack of Documentation for Service Design Decisions

📌 **Clause: 8.1 – SMS Planning**

What's going wrong:
Design decisions — such as technology choices, supplier selection, or service architecture — are made but not documented or justified.

Why it matters during an ISO 20000 audit:
Auditors assess transparency and traceability of decision-making in service planning.

How to fix it:
✓ Maintain a service design record template
✓ Log key decisions, rationale, and risk assessments
✓ Store documentation with change or project records

Real-world result:
Documented design history improves accountability, facilitates knowledge transfer, and supports compliance.

93. Security Controls Are Not Linked to Service Management Processes

📌 **Clause: 6.1 & 8.1 – Risk and Process Planning**

What's going wrong:
Security controls (e.g., access, logging, encryption) are managed by IT security teams but disconnected from SMS controls and documentation.

Why it matters during an ISO 20000 audit:
Auditors look for integration of risk and security within service processes. Silos increase operational and compliance risk.

How to fix it:

✓ Identify SMS processes that involve or depend on security

✓ Document how controls are implemented (e.g., in change, incident, asset management)

✓ Link to ISO/IEC 27001 where relevant

Real-world result:
Security-SMS alignment ensures holistic risk management and satisfies cross-standard compliance goals.

94. No Review of Service Dependencies During Supplier Changes

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
When switching or modifying vendors, service dependencies and business impact aren't re-evaluated, risking disruption.

Why it matters during an ISO 20000 audit:
Auditors expect continuity of service during supplier transitions. Lack of dependency review increases delivery risk.

How to fix it:

✓ Conduct impact and dependency analysis before approving supplier changes

✓ Update CMDB and risk register accordingly

✓ Review new supplier agreements against service requirements

Real-world result:
Dependency-aware transitions improve stability and reduce surprise service degradation.

95. Risk Treatments Are Not Tracked to Closure

📌 **Clause: 6.1 – Actions to Address Risks and Opportunities**

What's going wrong:
Risks are identified and treatments are proposed — but no one checks if mitigation actions were completed or effective.

Why it matters during an ISO 20000 audit:
Auditors expect a full risk lifecycle — from identification through resolution.

How to fix it:
✓ Add treatment tracking columns to your risk register (owner, due date, status, effectiveness)
✓ Review open treatments in regular risk meetings
✓ Verify effectiveness and document the outcome

Real-world result:
Treatment tracking closes the loop and strengthens risk governance maturity.

96. No Defined Retention Periods for SMS Records

📌 **Clause: 7.5 – Documented Information**

What's going wrong:
Records like incident logs, audit results, and service reports are stored indefinitely — or deleted without policy, risking legal and audit issues.

Why it matters during an ISO 20000 audit:
Auditors expect defined, enforced retention rules to support transparency and compliance.

How to fix it:

✓ Define record retention timelines by document type

✓ Align with legal, regulatory, and business requirements

✓ Automate archive or deletion where possible

Real-world result:
Structured recordkeeping reduces risk and supports data hygiene, especially during audits or legal inquiries.

97. Access Rights for SMS Tools Are Not Reviewed

📌 **Clause: 7.2 – Competence and Security Awareness**

What's going wrong:
Former staff or reassigned employees still have admin access to ITSM platforms, CMDBs, or service dashboards.

Why it matters during an ISO 20000 audit:
Access control is a key component of SMS integrity. Auditors expect periodic reviews for access appropriateness.

How to fix it:

✓ Review access to SMS-related tools quarterly

✓ Link access rights to role changes and offboarding procedures

✓ Maintain logs of reviews and access changes

Real-world result:
Proper access management protects SMS integrity and reduces both compliance and security risks.

98. Suppliers Are Not Involved in Change or Incident Resolution

📌 **Clause: 8.6 – Supplier Management**

What's going wrong:
When incidents or changes involve third-party components, vendors are not engaged in time, delaying resolution.

Why it matters during an ISO 20000 audit:
Auditors assess service continuity and vendor integration. Siloed supplier handling weakens service responsiveness.

How to fix it:
✓ Involve suppliers in change evaluations and incident escalations where applicable
✓ Define response timelines in contracts and SLAs
✓ Track supplier participation in service reports

Real-world result:
Vendor engagement improves responsiveness, supports SLAs, and reinforces end-to-end accountability.

99. No Escalation Process for Service Management Issues Beyond IT

📌 **Clause: 5.3 & 8.5 – Governance and Relationship Management**

What's going wrong:
When serious SMS issues arise (e.g., recurring SLA failures, customer disputes), there's no path to escalate beyond the IT team.

Why it matters during an ISO 20000 audit:
Auditors expect clear governance — including escalation to leadership if needed to resolve systemic service issues.

How to fix it:

✓ Define escalation points into senior management, legal, or customer success teams

✓ Document in governance or issue management procedures

✓ Review high-impact cases in management reviews

Real-world result:
Cross-functional escalation ensures serious issues are resolved holistically and swiftly.

100. No Periodic Review of the SMS as a Whole

📌 **Clause: 9.3 – Management Review**

What's going wrong:
Processes are reviewed in isolation, but there's no holistic review of the SMS's effectiveness, scope, and strategic alignment.

Why it matters during an ISO 20000 audit:
Management review is a cornerstone of the standard. Without it, auditors may view your SMS as fragmented or stagnant.

How to fix it:

✓ Schedule full SMS reviews annually with leadership

✓ Include performance, risk, improvement, feedback, and scope topics

✓ Document decisions and assigned actions

Real-world result:
Comprehensive reviews keep your SMS effective, aligned, and continually improving.

Strengthening Your ISO 20000 Compliance Journey

Achieving and maintaining ISO/IEC 20000 certification is more than passing an audit — it's about building a service management system that delivers consistent value, supports business continuity, and earns stakeholder trust.

By identifying and addressing these 100 common non-conformities, your organization isn't just checking boxes — you're creating a scalable, resilient, and customer-aligned ITSM framework.

Continuous Improvement is Essential
Service quality is not static. Regular audits, customer feedback, KPI reviews, and process refinements are critical to keeping your SMS relevant and responsive to evolving business demands.

Governance and Accountability Matter
Track ownership of processes, risks, and supplier relationships. Maintain updated records, monitor compliance, and enforce role-based responsibilities to build a robust and auditable SMS.

Turn Service Excellence Into Strategic Advantage
A well-implemented Service Management System not only ensures service reliability and compliance — it also improves customer satisfaction, enables operational efficiency, and supports competitive differentiation.

Use this guide as your practical reference for driving maturity, avoiding audit setbacks, and building a high-performance service environment. Stay proactive, stay reliable — and let ISO 20000 fuel your journey to world-class IT service delivery.

GSDC
Global Skill Development Council

CERTIFIED ISO 20000:2018 LEAD AUDITOR

ISO 20000 Lead Auditor 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

- **Assess organizations' compliance with ISO 20000.**
- **Ensure effective implementation of ISO 20000 standards.**
- **Evaluate risks associated with ISO 20000.**
- **Demonstrate proficiency in IT service management auditing.**

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

Enroll Now

www.gsdcouncil.org