Top 100 ISO/IEC 19770-1 Lead Auditor Audit Failures (And How to Avoid Them)

A Comprehensive Guide to Strengthening IT Asset Management Compliance

About This Guide

As organizations grow more reliant on software, hardware, and cloud-based platforms, managing IT assets effectively has become a critical component of business performance, cost control, and risk mitigation. ISO/IEC 19770-1 provides a globally recognized framework for IT Asset Management (ITAM) — one that prioritizes governance, lifecycle visibility, and audit-readiness.

But achieving and maintaining certification isn't always easy.

This guide has been compiled after extensive interviews with **over 100 ISO/IEC 19770-1 Lead Auditors**, dozens of real-world audit reports, and documented internal audit failures across industries. The goal? To help you **anticipate, prevent, and correct the most common ITAM audit non-conformities** — before they delay or derail your compliance journey.

Whether you're preparing for initial certification, performing an internal audit, or supporting your organization through a surveillance audit, this survival kit is your go-to tool for proactive compliance.

Objectives of This Guide

✓ Identify the most frequent and high-risk non-conformities observed during ISO/IEC 19770-1 audits
✓ Provide clause-based mapping of issues to help teams address gaps with precision
✓ Deliver clear, actionable solutions and corrective guidance for each non-conformity
✓ Enhance internal audit preparedness and improve system maturity

✓ Support IT asset managers, compliance officers, and auditors in building a reliable, scalable, and secure ITAM system

Who Should Use This Guide

- **IT Asset Management Teams** developing or auditing their ISO/IEC 19770-1 systems
- **IT Compliance & Risk Officers** ensuring alignment with IT governance frameworks
- **Procurement, Finance, and Vendor Managers** working with software licensing and hardware lifecycles
- **ITSM, Configuration Management, and Service Desk Leads** integrating CMDB and ITAM processes
- **Lead Auditors and Consultants** preparing organizations for ISO/IEC 19770-1 certification or re-certification

How This Guide Is Structured

Each non-conformity is presented using a clear, repeatable format:

- 📌 **Clause Reference** – Aligned with ISO/IEC 19770-1 sections
- **What's Going Wrong** – A concise description of the audit failure or system weakness
- **Why It Matters During an Audit** – The auditor's perspective and associated compliance risks
- **How to Fix It** – Practical steps to resolve the issue and strengthen the system

- **Real-World Result** – Expected outcomes from implementing the fix

The guide is organized in sets of ten non-conformities to allow focused reviews and team-based improvement sessions.

1. No Formal IT Asset Management Policy

📌 **Clause:** 5.1 – Leadership and Commitment

What's Going Wrong:
Organizations may track assets, but they operate without a documented ITAM policy outlining governance, objectives, and scope.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a clear policy to demonstrate leadership commitment and a structured approach. Auditors view its absence as a governance failure.

How to Fix It:

✓ Draft a formal ITAM policy approved by senior management

✓ Define scope, objectives, roles, and performance expectations

✓ Communicate the policy organization-wide and review annually

Real-World Result:
Improved leadership engagement and a clear foundation for audit scope, process control, and compliance.

2. Unclear Roles and Responsibilities

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

What's Going Wrong:
There is confusion over who is responsible for asset discovery, license reconciliation, lifecycle oversight, and data governance.

Why It Matters During an Audit:
Without defined accountability, ISO/IEC 19770-1 controls break down. Auditors expect documented role assignments.

How to Fix It:

✓ Develop a RACI matrix mapping all ITAM processes to responsible roles

✓ Update job descriptions and assign named owners

✓ Review and revise as teams or systems evolve

Real-World Result:
Reduced ambiguity, improved control execution, and faster audit readiness.

3. No Centralized Asset Inventory

📌 **Clause:** 8.1 – Planning and Control of Asset Management Processes

What's Going Wrong:
Assets are tracked in silos by different departments or systems. There is no single source of truth.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires centralized, accurate, and complete inventory data. Fragmentation undermines traceability and control.

How to Fix It:

✓ Consolidate asset records across IT, procurement, and finance

✓ Implement automated discovery tools and integrate data feeds

✓ Reconcile records monthly and assign inventory owners

Real-World Result:
Increased inventory accuracy, better lifecycle control, and simplified audits.

4. Incomplete Software License Records

📌 **Clause:** 8.3 – Software Asset Management Controls

What's Going Wrong:
License entitlements are stored in contracts or spreadsheets with no linkage to installed software or usage data.

Why It Matters During an Audit:
Auditors assess whether entitlements match usage. Missing records result in non-compliance or overspending.

How to Fix It:
✓ Maintain a centralized license entitlement repository
✓ Map entitlements to installations and usage data
✓ Conduct quarterly reconciliation reviews

Real-World Result:
Reduced financial risk, audit exposure, and unlicensed software use.

5. Asset Lifecycle Processes Not Defined

📌 **Clause:** 8.2 – Lifecycle Processes

What's Going Wrong:
No standard procedures exist for onboarding, refreshing, redeploying, or disposing of IT assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects repeatable lifecycle management. Gaps create security, cost, and compliance issues.

How to Fix It:

✓ Document processes for all lifecycle stages

✓ Align with ITSM, procurement, and information security

✓ Train staff and audit lifecycle logs annually

Real-World Result:
Improved resource planning and smoother integration across business units.

6. No Asset Risk Classification Model

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

What's Going Wrong:
All assets are treated equally regardless of value, criticality, or data sensitivity.

Why It Matters During an Audit:
Risk-based controls are essential in ISO/IEC 19770-1. Auditors look for differentiated treatment of high-impact assets.

How to Fix It:

✓ Develop risk criteria and classify assets by business function and sensitivity

✓ Map critical assets to enhanced monitoring and control measures

✓ Reassess classifications during lifecycle events

Real-World Result:
Stronger alignment with IT risk management and data protection frameworks.

7. Asset Discovery Tools Not Monitored

📌 **Clause:** 7.2 – Competence and Operational Control

What's Going Wrong:
Discovery agents are deployed but not maintained, leading to outdated or partial asset data.

Why It Matters During an Audit:
ISO/IEC 19770-1 demands accurate, timely inventory. Inactive tools create data gaps and undermine reliability.

How to Fix It:

✓ Monitor agent health, deployment rates, and scan frequency

✓ Implement alerts for inactive or missing agents

✓ Review discovery coverage during internal audits

Real-World Result:
More complete asset visibility and fewer blind spots in ITAM processes.

8. CMDB and Asset Register Not Integrated

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
Configuration data (e.g., in ITSM systems) is not synchronized with the asset register, creating duplication and mismatches.

Why It Matters During an Audit:
Auditors look for alignment between ITAM and ITSM systems. Inconsistencies cause audit flags and operational confusion.

How to Fix It:

✓ Link configuration items to asset records using unique identifiers

✓ Conduct quarterly reconciliation between CMDB and asset register

✓ Align updates with change and incident processes

Real-World Result:

Improved change control, incident response, and data consistency.

9. Disposal and Data Destruction Are Not Documented

📌 **Clause:** 8.2.6 – Retirement and Disposal

What's Going Wrong:

Assets are wiped or removed without chain of custody records, disposal logs, or destruction certificates.

Why It Matters During an Audit:

Disposal is a high-risk area. ISO/IEC 19770-1 requires evidence of secure and compliant end-of-life procedures.

How to Fix It:

✓ Establish secure disposal protocols and vendor SLAs

✓ Collect certificates of destruction or transfer documentation

✓ Audit disposal events for completeness

Real-World Result:

Reduced data leakage risk and improved compliance with data protection regulations.

10. No Regular Internal ITAM Audits Conducted

📌 **Clause:** 9.2 – Internal Audit

What's Going Wrong:
Organizations rely solely on annual external audits or certification reviews, with no internal self-assessment cycle.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires internal audits to monitor performance and identify areas for improvement.

How to Fix It:

✓ Develop an internal audit schedule based on risk and asset scope

✓ Train internal reviewers on ITAM and the ISO/IEC 19770-1 checklist

✓ Track audit findings and corrective actions in a central system

Real-World Result:
Early detection of gaps, better audit preparedness, and continual system improvement.

11. No Documented Objectives for the ITAM System

📌 **Clause:** 6.2 – ITAM Objectives and Planning

What's Going Wrong:
Organizations manage assets without defining measurable goals for cost control, compliance, risk, or performance improvement.

Why It Matters During an Audit:
Auditors require documented objectives to evaluate whether the ITAM system is aligned with business strategy and performance tracking.

How to Fix It:

✓ Set SMART objectives (e.g., reduce software audit risk by 30%)

✓ Align with strategic goals and update annually

✓ Review performance against objectives during management reviews

Real-World Result:
Clear direction for continuous improvement and stronger leadership engagement.

12. Lack of Awareness Training for Asset Management Roles

📌 **Clause:** 7.3 – Awareness

What's Going Wrong:
Stakeholders in IT, finance, or procurement are involved in asset decisions but unaware of ISO/IEC 19770-1 requirements or policies.

Why It Matters During an Audit:
Awareness training is mandatory for everyone whose actions impact the ITAM system. Gaps here weaken accountability and execution.

How to Fix It:

✓ Develop awareness modules for all asset-related roles

✓ Include policy overview, responsibilities, and compliance risks

✓ Track participation and update content annually

Real-World Result:
Stronger role alignment and fewer process breakdowns caused by misinformed teams.

13. Vendor Agreements Do Not Include ITAM Compliance Clauses

📌 **Clause:** 8.3.3 – Supplier and Contract Management

What's Going Wrong:
Contracts with hardware and software suppliers lack language about license tracking, audits, or asset return requirements.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects asset-related obligations to be governed in supplier agreements. Missing clauses create gaps in control.

How to Fix It:

✓ Review vendor templates and update with ITAM-specific terms

✓ Involve legal, procurement, and ITAM during contract negotiation

✓ Maintain a list of contract terms relevant to audit and compliance

Real-World Result:
Reduced vendor risk and greater control over asset-related obligations.

14. No Integration Between ITAM and Information Security Policies

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

What's Going Wrong:
Security and ITAM teams work independently, with no alignment on risk classifications, device controls, or asset tracking during incidents.

Why It Matters During an Audit:
Asset-related risks (e.g., data loss, software misuse) require joint mitigation. Misalignment indicates systemic governance issues.

How to Fix It:

✓ Coordinate asset classification with security risk frameworks

✓ Define joint controls (e.g., encryption, disposal, access)

✓ Share asset data for threat detection and vulnerability management

Real-World Result:

Stronger cyber resilience and improved audit performance across domains.

15. Cloud Assets Not Tracked in the Asset Register

📌 **Clause:** 8.1 – Asset Identification and Inventory

What's Going Wrong:

SaaS, PaaS, and cloud-based infrastructure are excluded from the ITAM system, leading to gaps in visibility and control.

Why It Matters During an Audit:

ISO/IEC 19770-1 covers all IT assets, including virtualized or cloud-based systems. Omission of cloud services is a growing audit failure.

How to Fix It:

✓ Define cloud asset categories and add to the inventory system

✓ Integrate data from cloud service portals or billing feeds

✓ Assign ownership and lifecycle controls to virtual assets

Real-World Result:

Improved governance and risk oversight for cloud-based environments.

16. Failure to Monitor Asset Performance and Value

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

What's Going Wrong:
Assets are tracked passively but not evaluated for ongoing performance, utilization, or return on investment.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes continual monitoring. Lack of performance metrics means missed cost-saving and improvement opportunities.

How to Fix It:

✓ Track utilization and maintenance costs for key assets

✓ Set performance thresholds to identify underused assets

✓ Report findings in regular management reviews

Real-World Result:
Optimized resource use and improved lifecycle planning.

17. Asset Records Lack Purchase and Warranty Information

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
The asset inventory captures basic details but omits purchase dates, supplier information, or warranty status.

Why It Matters During an Audit:
These details are critical for financial control, support decisions, and lifecycle governance. Incomplete records signal immaturity.

How to Fix It:

✓ Define mandatory asset data fields including financial and vendor details

✓ Populate missing data through reconciliation with procurement systems

✓ Automate data capture where possible

Real-World Result:

Better decision-making, contract leverage, and asset valuation.

18. No Software Metering or Usage Tracking Implemented

📌 **Clause:** 8.3 – Software Asset Management

What's Going Wrong:

Organizations deploy licenses but do not monitor usage, leading to over-purchasing or compliance risks from underutilization.

Why It Matters During an Audit:

Auditors expect usage data to support entitlement reconciliation. Without it, license data is unreliable.

How to Fix It:

✓ Deploy metering tools for all major software products

✓ Compare usage against entitlements regularly

✓ Decommission or reallocate underused licenses

Real-World Result:

Cost reduction and tighter license compliance.

19. No Corrective Action Process for Audit Findings

📌 **Clause:** 10.2 – Nonconformity and Corrective Action

What's Going Wrong:
Internal or external audit findings are recorded but not tracked, investigated, or closed out formally.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates corrective actions to address weaknesses. Lack of process indicates poor governance.

How to Fix It:

✓ Implement a centralized non-conformity log

✓ Assign corrective action owners and deadlines

✓ Review closure status in management reviews

Real-World Result:
Faster resolution of audit risks and demonstrable commitment to continual improvement.

20. Asset Records Not Archived or Controlled After Disposal

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
Disposed asset records are deleted or lost, making it impossible to prove proper disposal during future audits.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires document retention aligned with lifecycle processes. Missing records create audit exposure.

How to Fix It:

✓ Define retention periods for disposal documentation (e.g., 3–7 years)

✓ Store retired asset logs in secure archives

✓ Include disposal tracking in internal audits

Real-World Result:
Improved traceability, legal defensibility, and audit confidence.

21. ITAM Objectives Not Linked to Business Strategy

📌 **Clause:** 6.2 – ITAM Objectives and Planning

What's Going Wrong:
Objectives for the ITAM system are created in isolation, without alignment to broader business goals such as cost optimization, sustainability, or risk reduction.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires objectives to support the organization's strategic direction. Misalignment limits relevance and effectiveness.

How to Fix It:

✓ Involve senior leadership in objective-setting

✓ Link ITAM metrics to business KPIs and risk frameworks

✓ Communicate the alignment in management reviews

Real-World Result:
Stronger leadership engagement and greater investment in ITAM maturity.

22. Manual Data Entry Causes Frequent Inventory Errors

📌 **Clause:** 8.1 – Planning and Control of Asset Management Processes

What's Going Wrong:
Asset inventory relies on spreadsheets or forms with no automation, leading to outdated, duplicated, or inaccurate data.

Why It Matters During an Audit:
Accuracy and completeness of records are foundational. Manual errors reduce reliability and increase audit risk.

How to Fix It:

✓ Automate data capture through discovery tools and integration

✓ Set up validation rules and alerts for inconsistent data

✓ Audit asset records quarterly for accuracy

Real-World Result:
Reduced inventory errors and more efficient audit preparation.

23. Software Installation Procedures Are Uncontrolled

📌 **Clause:** 8.3 – Software Asset Management

What's Going Wrong:
Employees can install software without approval, metering, or reconciliation, resulting in shadow IT and unmanaged risk.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires software deployment to be controlled and aligned with entitlements.

How to Fix It:

✓ Enforce installation controls via service desk or self-service portals

✓ Validate new installations against licensing agreements

✓ Monitor for unauthorized software regularly

Real-World Result:
Stronger license compliance and fewer vendor audit liabilities.

24. Hardware Assets Lack Assigned Business Owners

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

What's Going Wrong:
IT or operations manage assets, but ownership is unclear, particularly for end-user devices or shared infrastructure.

Why It Matters During an Audit:
Accountability is a core ISO/IEC 19770-1 requirement. Unassigned assets increase loss risk and weaken lifecycle control.

How to Fix It:

✓ Assign named business owners for every asset category

✓ Include ownership during onboarding and assignment workflows

✓ Review ownership during audits or inventory updates

Real-World Result:
Improved control, faster issue resolution, and reduced asset loss.

25. Asset Management Not Included in Change Control Process

📌 **Clause:** 8.2.5 – Maintenance and Modification

What’s Going Wrong:
Assets are modified or replaced without updating records, especially during IT changes or upgrade projects.

Why It Matters During an Audit:
Uncontrolled changes create data mismatches and break lifecycle traceability, breaching ISO/IEC 19770-1 expectations.

How to Fix It:

✓ Integrate ITAM checkpoints into change management workflows

✓ Update asset records as part of change implementation

✓ Require post-change reconciliation for critical assets

Real-World Result:
Fewer inventory inaccuracies and better lifecycle continuity.

26. No Policy for Handling Orphaned or Unused Assets

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

What’s Going Wrong:
Unused hardware and licenses remain in the system with no procedure for reassignment, redeployment, or disposal.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects control of all assets throughout their lifecycle, including those not actively in use.

How to Fix It:

✓ Implement regular reviews of asset utilization

✓ Define thresholds for inactivity and disposal

✓ Include orphaned asset handling in lifecycle documentation

Real-World Result:

Reduced waste, lower costs, and clearer asset tracking.

27. Incomplete Documentation of Software Contracts and Terms

📌 **Clause:** 8.3.3 – Software License Management

What's Going Wrong:

Contract details such as license caps, renewal terms, or usage restrictions are not recorded or linked to asset data.

Why It Matters During an Audit:

Auditors check for entitlement-to-usage alignment. Missing contract data limits your ability to defend against non-compliance.

How to Fix It:

✓ Store all contracts and entitlements in a central repository

✓ Extract key licensing terms and link them to asset records

✓ Involve legal or procurement in validation

Real-World Result:

Clearer license tracking and reduced risk of vendor disputes.

28. No Controls for BYOD (Bring Your Own Device) Environments

📌 **Clause:** 8.1 – Asset Identification and Scope

What's Going Wrong:
Employees use personal devices for work-related tasks, but these devices are not inventoried or governed under ITAM processes.

Why It Matters During an Audit:
Untracked devices accessing business systems increase data security and asset visibility risks.

How to Fix It:
✓ Define a BYOD policy and acceptable use standards
✓ Track authorized BYOD devices in a separate registry
✓ Apply minimum security controls and monitoring

Real-World Result:
Improved security, better compliance, and reduced shadow IT exposure.

29. Lack of Version Control on ITAM Documentation

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
ITAM procedures and policies are updated informally without versioning or approval workflows.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates document control to ensure consistency and accuracy of operational processes.

How to Fix It:

✓ Use version control systems for all policies and procedures

✓ Require approval and publication dates on each document

✓ Store current and archived versions in a controlled location

Real-World Result:
Improved auditability and stronger governance of operational documentation.

30. No Metrics for Measuring ITAM System Performance

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

What's Going Wrong:
ITAM activities are performed, but no KPIs or metrics are tracked to evaluate effectiveness or improvement.

Why It Matters During an Audit:
Without performance data, auditors cannot verify system maturity or compliance effectiveness.

How to Fix It:

✓ Define KPIs such as inventory accuracy, license utilization, and reconciliation frequency

✓ Report metrics in monthly or quarterly reviews

✓ Adjust controls based on trends and findings

Real-World Result:
Stronger operational visibility and data-driven continuous improvement.

31. ITAM System Not Reviewed in Management Reviews

📌 **Clause:** 9.3 – Management Review

What's Going Wrong:
Top management does not formally review ITAM system performance, risks, or opportunities as part of scheduled management reviews.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires management involvement and periodic review. Its absence implies weak oversight and lack of strategic direction.

How to Fix It:

✓ Include ITAM performance, objectives, audit findings, and risk updates in the management review agenda

✓ Document review outcomes and follow-up actions

✓ Conduct reviews at least annually

Real-World Result:
Stronger executive engagement and alignment with organizational goals.

32. Software Installations Not Verified Post-Deployment

📌 **Clause:** 8.3 – Software Asset Management

What's Going Wrong:
After deployment, there is no validation that installed software matches approved entitlements or intended versions.

Why It Matters During an Audit:
Unverified deployments increase the risk of non-compliance, licensing issues, and compatibility problems.

How to Fix It:

✓ Implement post-installation checks using metering or discovery tools

✓ Compare installed versions with procurement and license data

✓ Include verification in the software request workflow

Real-World Result:
Improved license control and minimized configuration-related incidents.

33. ITAM Risks Not Documented in Risk Register

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

What's Going Wrong:
Asset-related risks (e.g., hardware loss, software misuse, vendor lock-in) are managed informally and not captured in the enterprise risk register.

Why It Matters During an Audit:
Risk awareness and treatment must be documented to demonstrate compliance and due diligence.

How to Fix It:

✓ Work with the risk team to assess and log ITAM risks

✓ Define mitigation actions and control ownership

✓ Review risks during internal audits and management meetings

Real-World Result:
Greater visibility and accountability for asset-related risks.

34. Asset Requests and Allocations Not Tracked Centrally

📌 **Clause:** 8.2 – Lifecycle Processes

What's Going Wrong:
Devices are assigned based on ad hoc requests, and there's no system to track who has what or when it was issued.

Why It Matters During an Audit:
Lack of issuance tracking can lead to asset loss, duplication, and noncompliance with lifecycle controls.

How to Fix It:

✓ Use an ITSM or asset request platform with tracking features

✓ Require user acknowledgment at assignment

✓ Reconcile assigned vs. returned assets monthly

Real-World Result:
Reduced asset loss and more reliable user-device mapping.

35. No Defined Criteria for Asset Criticality

📌 **Clause:** 6.1 – Risk-Based Classification

What's Going Wrong:
Asset importance is subjective. Teams use inconsistent criteria for deciding what is "critical" or "non-essential."

Why It Matters During an Audit:
ISO/IEC 19770-1 calls for documented, risk-based prioritization of asset controls.

How to Fix It:

✓ Develop a scoring model based on data sensitivity, operational role, or legal impact

✓ Apply classifications consistently across the inventory

✓ Align control levels with asset tiering

Real-World Result:
More efficient resource use and targeted monitoring of key assets.

36. ITAM Responsibilities Are Not Covered in Onboarding

📌 **Clause:** 7.2 – Competence

What's Going Wrong:
New employees, including IT staff and procurement personnel, are not briefed on asset handling responsibilities during onboarding.

Why It Matters During an Audit:
Roles affecting ITAM must be competent and trained. Failure to onboard correctly leads to early-stage control breakdowns.

How to Fix It:

✓ Include ITAM policy, lifecycle steps, and tool usage in onboarding content

✓ Assign refresher training timelines

✓ Validate understanding during probation reviews

Real-World Result:
Increased compliance and fewer errors from role misunderstanding.

37. Assets Not Tagged or Physically Identified

📌 **Clause:** 8.1 – Asset Identification and Labeling

What's Going Wrong:
Many physical assets (especially peripherals and remote devices) lack tags or barcodes, making them hard to trace or reconcile.

Why It Matters During an Audit:
Physical identification supports location, verification, and ownership control—key requirements in the ISO/IEC 19770-1 checklist.

How to Fix It:

✓ Tag all new assets at the point of provisioning

✓ Include asset IDs in all ITAM systems

✓ Conduct periodic physical audits

Real-World Result:
Better audit traceability and less asset-related confusion during redeployment or retirement.

38. License Renewals and Expirations Are Not Proactively Managed

📌 **Clause:** 8.3.3 – License Management

What's Going Wrong:
License terms and renewal dates are managed reactively, often leading to overspending or last-minute decisions.

Why It Matters During an Audit:
Unplanned renewals can create compliance gaps or budget surprises. ISO/IEC 19770-1 expects proactive control.

How to Fix It:

✓ Maintain a license calendar with alerts 60–90 days in advance

✓ Review usage prior to renewal for optimization

✓ Store renewal logs and documentation centrally

Real-World Result:

More strategic license management and lower costs.

39. Inconsistent Asset Categorization Across Systems

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:

One system may list a device as a laptop, while another calls it a workstation. Categories are not standardized across platforms.

Why It Matters During an Audit:

Misaligned data creates reconciliation issues, erodes confidence, and complicates audit traceability.

How to Fix It:

✓ Define and standardize asset categories (e.g., laptop, server, router)

✓ Apply the same taxonomy across all inventory systems

✓ Validate consistency through automated or manual audits

Real-World Result:

Streamlined reporting, better analytics, and reduced duplication.

40. Vendor Asset Returns Not Monitored Post-Termination

📌 **Clause:** 8.2.6 – Disposal and Return

What's Going Wrong:
Leased or vendor-managed assets are not tracked after contract termination. Returns may be missed or undocumented.

Why It Matters During an Audit:
Failure to prove asset return or disposal can result in financial penalties or security risks.

How to Fix It:
✓ Track vendor-owned asset locations and return deadlines
✓ Require return receipts or certificates of return
✓ Monitor compliance with vendor SLAs

Real-World Result:
Avoided penalties, lower residual risk, and greater accountability with third parties.

41. No Controls for Deactivated or Inactive Assets

📌 **Clause:** 8.2.4 – Monitoring and Control of Assets

What's Going Wrong:
Assets that are powered off, disconnected, or inactive for long periods are not monitored or flagged for review.

Why It Matters During an Audit:
Inactive assets can be stolen, repurposed without approval, or left vulnerable. ISO/IEC 19770-1 requires oversight even when not in daily use.

How to Fix It:

✓ Define inactivity thresholds (e.g., 90 days)

✓ Flag and investigate assets with no activity

✓ Review status before reassignment or disposal

Real-World Result:

Improved asset accountability and reduced risk of misuse or data exposure.

42. Procurement Processes Are Not Linked to ITAM Records

📌 **Clause:** 8.2.1 – Acquisition and Registration of Assets

What's Going Wrong:

Purchased assets are not automatically recorded in the ITAM system, resulting in missing or delayed records.

Why It Matters During an Audit:

Auditors expect a traceable link between procurement and asset records. Manual handovers often cause errors or omissions.

How to Fix It:

✓ Integrate ITAM tools with procurement platforms

✓ Auto-populate new asset entries from purchase data

✓ Review reconciliation reports monthly

Real-World Result:

Stronger lifecycle visibility and improved audit alignment.

43. No Secure Disposal of Electronic Storage Media

📌 **Clause:** 8.2.6 – Disposal

What's Going Wrong:
Hard drives, USBs, and other storage media are discarded without formal wiping, encryption, or tracking.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires data-bearing assets to be disposed of securely. Failing this can breach privacy laws and corporate policies.

How to Fix It:

✓ Use certified data destruction services

✓ Log all data wipes and maintain destruction certificates

✓ Include disposal requirements in ITAM and security policies

Real-World Result:
Improved data protection and legal compliance.

44. No User Acknowledgment for Issued Assets

📌 **Clause:** 8.2.2 – Assignment and Use

What's Going Wrong:
Employees receive laptops or phones without signing forms or acknowledging terms of use.

Why It Matters During an Audit:
Unacknowledged assets reduce accountability. ISO/IEC 19770-1 expects user agreement for tracking, use, and policy compliance.

How to Fix It:

✓ Implement asset handover forms or digital acknowledgment

✓ Include use policy and return conditions

✓ Store signed records in the ITAM system

Real-World Result:

Higher responsibility among users and smoother return processes.

45. Shadow IT Assets Not Identified or Managed

📌 **Clause:** 8.1 – Asset Scope and Discovery

What's Going Wrong:

Employees acquire software or devices independently, bypassing ITAM systems, leading to hidden risks and non-compliance.

Why It Matters During an Audit:

ISO/IEC 19770-1 mandates full visibility over all IT assets. Shadow IT undermines security, license compliance, and data governance.

How to Fix It:

✓ Use network monitoring tools to detect unmanaged assets

✓ Educate employees on procurement policies

✓ Regularly audit system access and usage

Real-World Result:

Tighter control over unauthorized tools and improved audit defense.

46. Leased Equipment Not Monitored for End-of-Term Returns

📌 **Clause:** 8.2.6 – Lifecycle Closure and Return

What's Going Wrong:
Organizations lease equipment but fail to track return deadlines or residual terms, risking late fees or asset loss.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires control over all asset types, including leased equipment.

How to Fix It:
✓ Track lease terms in your asset register
✓ Set alerts for return and renewal dates
✓ Reconcile returned items with vendor records

Real-World Result:
Avoided penalties and improved financial and inventory accuracy.

47. No Controls for Privileged Software (e.g., Admin Tools)

📌 **Clause:** 8.3 – Software Controls

What's Going Wrong:
Admin tools, compilers, and diagnostic software are installed without usage restrictions or audit trails.

Why It Matters During an Audit:
Unauthorized use can lead to system compromise or misuse. ISO/IEC 19770-1 expects oversight of sensitive software assets.

How to Fix It:

✓ Create a privileged software category

✓ Restrict installation to approved users

✓ Audit usage and log all activity

Real-World Result:

Improved security posture and better compliance with IT governance frameworks.

48. Configuration Changes Not Reflected in Asset Records

📌 **Clause:** 8.2.5 – Maintenance and Updates

What's Going Wrong:

Device upgrades or hardware swaps are made without updating the asset record (e.g., RAM, hard drives, serial numbers).

Why It Matters During an Audit:

Accurate records are essential for inventory, support, and risk control. Auditors expect full traceability.

How to Fix It:

✓ Include ITAM updates in change or maintenance workflows

✓ Require technicians to log changes immediately

✓ Audit randomly for verification

Real-World Result:

Improved record integrity and faster resolution of configuration-based incidents.

49. SaaS Usage Not Aligned with Subscription Terms

📌 **Clause:** 8.3 – Software Asset Management

What's Going Wrong:
SaaS tools (e.g., Adobe, Microsoft 365) are underutilized or exceed subscription terms, leading to waste or compliance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 treats cloud-based software the same as on-premises. Misalignment risks vendor penalties or overpayment.

How to Fix It:

✓ Track active users and entitlements

✓ Analyze usage metrics regularly

✓ Adjust licenses or downgrade plans where needed

Real-World Result:
Lower SaaS costs and better license optimization.

50. Asset Records Not Aligned with Financial Depreciation Schedules

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
Finance teams and ITAM use different timelines for depreciation and lifecycle tracking, causing inconsistencies in value reporting.

Why It Matters During an Audit:
Auditors look for alignment between physical assets and financial records. Discrepancies suggest mismanagement.

How to Fix It:

✓ Align ITAM and finance asset categories and timelines

✓ Integrate ITAM tools with ERP systems where feasible

✓ Conduct periodic reconciliation

Real-World Result:
Stronger financial compliance and easier audit sign-offs.

51. Asset Management Scope Not Clearly Defined

📌 **Clause:** 4.3 – Determining the Scope of the ITAM System

What's Going Wrong:
Organizations attempt to manage "everything" without clearly defining what types of assets, systems, or departments fall within the ITAM system boundary.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a documented and justified scope. Vague or overly broad scopes create confusion and dilute accountability.

How to Fix It:

✓ Define scope based on asset types (hardware, software, SaaS, cloud) and organizational coverage

✓ Justify exclusions and document them in your ITAM plan

✓ Review the scope during each management review cycle

Real-World Result:
Sharper focus, improved compliance, and better resource planning.

52. Software Reallocation Process Is Not Standardized

📌 **Clause:** 8.3 – License Management and Optimization

What's Going Wrong:
When employees leave, software is rarely reassigned or deactivated. Licenses remain unused or continue to accrue costs.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes cost efficiency and control. Wasted entitlements lead to overspending and compliance issues.

How to Fix It:

✓ Include license reallocation in the offboarding process

✓ Use asset management tools to track active vs. inactive use

✓ Periodically review licenses for potential re-use

Real-World Result:
Optimized software spend and improved control over entitlements.

53. Lack of Metrics for Audit Closure and Corrective Actions

📌 **Clause:** 10.2 – Nonconformity and Corrective Action

What's Going Wrong:
Corrective actions from audits are tracked informally or inconsistently, with no measurement of closure time or impact.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects a defined and effective process for addressing audit findings. Without metrics, effectiveness is unclear.

How to Fix It:

✓ Set KPIs for corrective action closure (e.g., % closed in 30 days)

✓ Track resolution status in a central system

✓ Review during internal audits and management reviews

Real-World Result:

Faster resolution of weaknesses and better continuous improvement tracking.

54. No Review of ITAM Policies After Major System Changes

📌 **Clause:** 5.1 / 6.3 – Governance and Change Planning

What's Going Wrong:

New IT tools or sourcing models (e.g., cloud-first, remote work) are introduced without revisiting ITAM policies or controls.

Why It Matters During an Audit:

Standards require ITAM governance to remain relevant. Auditors expect policies to reflect current systems and practices.

How to Fix It:

✓ Trigger policy reviews during major IT or sourcing changes

✓ Document amendments and approval dates

✓ Communicate updates to all affected stakeholders

Real-World Result:

Greater policy relevance and reduced operational misalignment.

55. No Designated Point of Contact for Asset-Related Issues

📌 **Clause:** 5.3 – Roles and Responsibilities

What's Going Wrong:
Employees do not know who to contact for asset returns, reassignments, or clarifications, leading to unmanaged changes.

Why It Matters During an Audit:
Defined responsibility is central to ISO/IEC 19770-1. Unclear contact points increase risk and delay issue resolution.

How to Fix It:

✓ Designate role-based contacts for key asset categories

✓ Publish a responsibility matrix on internal portals

✓ Include escalation paths for exceptions

Real-World Result:
Faster asset resolution and better governance visibility.

56. No Lifecycle Controls for Mobile Devices

📌 **Clause:** 8.2 – Lifecycle Planning

What's Going Wrong:
Phones and tablets are issued without formal lifecycle documentation, often remaining in use beyond support or security timelines.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires documented lifecycle stages. Mobile devices are often overlooked, creating compliance risks.

How to Fix It:

✓ Include mobile assets in all ITAM lifecycle documentation

✓ Define refresh cycles and end-of-life criteria

✓ Monitor usage and OS support compliance

Real-World Result:
Stronger mobile governance and reduced operational and data risks.

57. No Record of Historical Asset Ownership

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
Ownership history is overwritten with each change. It's impossible to trace who had an asset during specific periods.

Why It Matters During an Audit:
Auditors may request historical ownership for investigations or compliance tracking. Lack of audit trails is a concern.

How to Fix It:

✓ Enable historical tracking in asset records

✓ Log changes with time stamps and user IDs

✓ Retain records per legal or policy retention timelines

Real-World Result:
Improved traceability and audit support in incident investigations.

58. ITAM Roles Not Included in Competency Frameworks

📌 **Clause:** 7.2 – Competence

What's Going Wrong:
ITAM-specific roles such as Asset Coordinator or License Manager are not included in HR-defined competency or skills matrices.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires evidence of role-specific training and skill verification.

How to Fix It:
✓ Define ITAM competencies and link to each job role
✓ Assess individuals against role expectations
✓ Provide targeted training and development plans

Real-World Result:
Stronger role performance and better audit defense on personnel competence.

59. Asset Statuses Are Vague or Inconsistent

📌 **Clause:** 8.1 – Asset Record Integrity

What's Going Wrong:
Assets are marked as "active," "on hold," or "other" with no clear definitions, leading to confusion and improper treatment.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes accurate, complete asset records. Ambiguous statuses hinder lifecycle planning.

How to Fix It:

✓ Standardize status options (e.g., active, deployed, retired, lost)

✓ Define each status in a data dictionary

✓ Train teams on status assignment

Real-World Result:

Better data quality and clearer asset insights across teams.

60. Performance of ITAM Tools Not Periodically Reviewed

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

What's Going Wrong:

The organization relies on legacy tools that no longer scale, integrate poorly, or fail to meet operational demands.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires tools to support effective control. Underperforming systems create audit risks and operational gaps.

How to Fix It:

✓ Conduct tool performance assessments annually

✓ Review feedback from end users and ITAM teams

✓ Upgrade or replace tools based on capability needs

Real-World Result:

Increased system efficiency, automation potential, and audit readiness.

61. Software Installations Lack Unique Asset Association

📌 **Clause:** 8.3 – Software Asset Management

What's Going Wrong:
Installed applications are not linked to specific hardware or user assets, making reconciliation and license tracking difficult.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires visibility of software use by device and user. Unlinked installations raise red flags for unauthorized or unmanaged use.

How to Fix It:
✓ Link each installed software record to a specific asset in the register
✓ Include user and device associations for all entitlements
✓ Audit quarterly for orphaned or unlinked applications

Real-World Result:
Improved entitlement tracking and software usage transparency.

62. Software Entitlements Are Not Reviewed After Vendor Changes

📌 **Clause:** 8.3.3 – License Management

What's Going Wrong:
When vendors update terms or move to subscription models, organizations fail to reassess their entitlements or compliance obligations.

Why It Matters During an Audit:
Vendor agreements evolve. ISO/IEC 19770-1 expects organizations to maintain current awareness of software rights and obligations.

How to Fix It:

✓ Monitor vendor updates and contract changes quarterly

✓ Involve ITAM in vendor management and renewal cycles

✓ Document reassessments and entitlement changes

Real-World Result:
Stronger compliance and proactive contract risk mitigation.

63. No Formalized Escalation Path for ITAM Issues

📌 **Clause:** 5.3 – Responsibility and Governance

What's Going Wrong:
When asset issues occur—such as losses or license breaches—there's no defined escalation process to report or resolve the problem.

Why It Matters During an Audit:
Auditors expect a formal, structured governance model with escalation procedures for nonconformities.

How to Fix It:

✓ Define escalation levels for incidents, discrepancies, and breaches

✓ Assign roles for each stage of response

✓ Communicate the process to IT, operations, and compliance

Real-World Result:
Faster issue resolution and improved incident traceability.

64. Configuration Baselines Are Not Maintained

📌 **Clause:** 8.2.5 – Maintenance and Configuration

What's Going Wrong:
Organizations do not document standard configurations (e.g., OS version, default applications) for different device types, leading to uncontrolled variance.

Why It Matters During an Audit:
ISO/IEC 19770-1 supports baseline management to enable monitoring, updates, and audit integrity.

How to Fix It:
✓ Establish and document configuration baselines per asset category
✓ Validate configurations during provisioning and support
✓ Periodically review and update baselines

Real-World Result:
Improved consistency and simplified audit and support procedures.

65. Virtual Assets Are Not Treated as Managed Assets

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Virtual machines, containers, and cloud-hosted systems are excluded from inventory and license oversight.

Why It Matters During an Audit:
All operational assets—physical or virtual—fall under ISO/IEC 19770-1. Exclusion creates blind spots.

How to Fix It:

✓ Identify and inventory all virtual and cloud-based systems

✓ Tag and track with appropriate metadata (host, lifecycle, purpose)

✓ Include in risk and license compliance reviews

Real-World Result:
More complete visibility and stronger alignment with hybrid environments.

66. No Validation Process for Vendor-Provided Asset Data

📌 **Clause:** 8.2.1 – Procurement Integration

What's Going Wrong:
Vendors or leasing companies supply asset records that are accepted without internal verification or cross-checking.

Why It Matters During an Audit:
Auditors expect independent validation to confirm accuracy. Errors in vendor data can cascade into compliance issues.

How to Fix It:

✓ Verify vendor records against physical delivery and system scans

✓ Use checklists during asset intake

✓ Document discrepancies and resolution steps

Real-World Result:
Higher data quality and fewer errors from third-party systems.

67. ITAM Training Programs Lack Measurable Outcomes

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

What's Going Wrong:
Training is delivered, but there are no post-training assessments, certifications, or measurement of on-the-job competency.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires competency—not just attendance. Auditors look for proof of learning effectiveness.

How to Fix It:

✓ Include quizzes or evaluations after all ITAM training

✓ Link training to job performance metrics

✓ Track ongoing development and certification progress

Real-World Result:
Better-qualified staff and measurable performance improvement.

68. Asset Recovery from Departing Employees Is Inconsistent

📌 **Clause:** 8.2.6 – Return and Recovery

What's Going Wrong:
Devices assigned to former employees are sometimes not returned, undocumented, or lost in handoff processes.

Why It Matters During an Audit:
Failure to recover assets weakens lifecycle control and inflates asset risks.

How to Fix It:

✓ Integrate asset return into HR offboarding workflows

✓ Require proof of return and inspection

✓ Escalate missing items using defined incident procedures

Real-World Result:
Lower asset loss and improved chain-of-custody documentation.

69. No Backup Plan for ITAM Tool Outages

📌 **Clause:** 6.1 – Risk Management

What's Going Wrong:
If the ITAM tool fails or is unavailable, there is no fallback plan for inventory access, license compliance checks, or provisioning workflows.

Why It Matters During an Audit:
Resilience is a key principle in ISO/IEC 19770-1. Tool dependency without contingency raises operational risk.

How to Fix It:

✓ Develop a documented contingency plan

✓ Maintain periodic offline backups or extracts

✓ Test recovery scenarios annually

Real-World Result:
Improved continuity and reduced tool-related disruption risks.

70. Policies Do Not Address Remote or Hybrid Asset Usage

📌 **Clause:** 5.2 / 6.3 – Policy and Planning

What's Going Wrong:
ITAM policies were written pre-remote work and do not account for home office setups, hybrid usage, or personal device access.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects policies to reflect the current operational reality. Gaps in remote governance increase compliance risk.

How to Fix It:

✓ Update policies to define rules for remote asset use

✓ Include security, tracking, and support conditions

✓ Train users and require acknowledgment

Real-World Result:
Stronger governance of distributed work environments and improved audit alignment.

71. No Standard Naming Convention for Asset Records

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Assets are entered into the system using inconsistent naming formats, causing confusion, duplication, and search errors.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires clear and traceable asset records. Poor naming conventions make lifecycle tracking difficult.

How to Fix It:

✓ Define a standard naming schema for hardware and software assets

✓ Apply format rules automatically in data entry forms

✓ Audit asset naming during routine data quality checks

Real-World Result:

Improved inventory clarity, faster data queries, and fewer duplicates.

72. No Internal KPI Reviews for ITAM Objectives

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

What's Going Wrong:

Although KPIs are defined for ITAM, performance data is not regularly reviewed, reported, or used to improve the system.

Why It Matters During an Audit:

Auditors expect evidence that objectives are being monitored. Ignoring KPIs shows weak management engagement.

How to Fix It:

✓ Schedule regular performance reviews against KPIs

✓ Document reviews in ITAM dashboards or management reports

✓ Use findings to adjust controls and improve processes

Real-World Result:

Greater accountability and continual improvement momentum.

73. Asset Reuse Guidelines Are Missing or Vague

📌 **Clause:** 8.2.2 – Reassignment and Reuse

What's Going Wrong:
Returned devices are either stockpiled or reissued without clear checks, resets, or condition evaluations.

Why It Matters During an Audit:
ISO/IEC 19770-1 promotes full lifecycle management. Informal reuse introduces security, reliability, and data risks.

How to Fix It:

✓ Create standard procedures for sanitizing and evaluating reused assets

✓ Track history and warranty status

✓ Require formal approvals before redeployment

Real-World Result:
Increased equipment value and more secure asset handovers.

74. Asset Verification Campaigns Are Not Conducted Periodically

📌 **Clause:** 9.1 – Asset Verification

What's Going Wrong:
Inventory is maintained but rarely validated through physical audits or user confirmations.

Why It Matters During an Audit:
Without verification, inventory accuracy declines. ISO/IEC 19770-1 requires regular validation to ensure data integrity.

How to Fix It:

✓ Conduct physical audits annually or by department rotation

✓ Use barcodes or check-in/out tools

✓ Compare audit findings with system records

Real-World Result:

Higher confidence in records and improved control accountability.

75. Software Request Workflows Are Not Aligned with Entitlements

📌 **Clause:** 8.3 – Software Lifecycle and Procurement

What's Going Wrong:

Employees request and install software without checking existing licenses or entitlements, leading to overspend.

Why It Matters During an Audit:

Software governance is a top priority for ISO/IEC 19770-1. Misalignment with entitlement data signals immature controls.

How to Fix It:

✓ Link approval workflows to entitlement databases

✓ Alert requesters and approvers if licenses already exist

✓ Flag recurring requests to optimize procurement

Real-World Result:

Reduced software waste and improved procurement coordination.

76. Asset Costs Are Not Tracked Beyond Procurement

📌 **Clause:** 8.2 – Lifecycle Cost Monitoring

What's Going Wrong:
Once purchased, assets are not tracked for ongoing costs like support contracts, repairs, or productivity losses.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes cost visibility over the full lifecycle. Ignoring downstream costs distorts ROI metrics.

How to Fix It:

✓ Track total cost of ownership (TCO) fields in asset records

✓ Include repair, support, and subscription data

✓ Use TCO trends in refresh or budgeting decisions

Real-World Result:
Better asset planning and more accurate financial insights.

77. End-of-Support Dates Not Monitored

📌 **Clause:** 8.2.5 – Maintenance and End-of-Life

What's Going Wrong:
Operating systems or software remain in use past their vendor support dates, exposing the organization to risk.

Why It Matters During an Audit:
Running unsupported software violates both security and compliance policies under ISO/IEC 19770-1.

How to Fix It:

✓ Record vendor support dates in asset metadata

✓ Set alerts for upcoming EOL milestones

✓ Plan upgrades or retirement in advance

Real-World Result:

Reduced security exposure and improved software lifecycle control.

78. Insufficient Documentation of Asset Changes

📌 **Clause:** 8.2.5 – Configuration and Maintenance

What's Going Wrong:

Changes to device configurations (e.g., OS upgrades, hardware swaps) are made without logging who made the change, when, or why.

Why It Matters During an Audit:

Auditors require change documentation to ensure traceability. Missing logs create integrity and accountability gaps.

How to Fix It:

✓ Log all changes in the ITAM or ITSM system

✓ Capture time stamps, user IDs, and change reasons

✓ Audit change history monthly

Real-World Result:

Improved audit trail, faster troubleshooting, and clearer accountability.

79. Software Installations Are Not Reconciled After Mergers or Acquisitions

📌 **Clause:** 8.3.3 – Entitlement and Risk Management

What's Going Wrong:
When organizations merge or acquire, duplicate or conflicting licenses remain unmanaged, causing overuse or violations.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects software license hygiene during integration events. Untouched portfolios increase audit and financial risk.

How to Fix It:

✓ Perform a full entitlement and deployment reconciliation

✓ Review license portability and merger clauses

✓ Consolidate contracts and remove redundancies

Real-World Result:
Reduced software spend and improved compliance alignment post-acquisition.

80. Cloud Asset Costs Not Linked to Business Units

📌 **Clause:** 8.1 / 9.1 – Cloud Inventory and Monitoring

What's Going Wrong:
Cloud usage is visible at the account level but not broken down by department, project, or user group, limiting cost ownership.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires cost traceability. Lack of cost attribution weakens financial governance and budgeting.

How to Fix It:

✓ Use tags or cost codes to allocate cloud resources

✓ Align usage with business units or functions

✓ Review usage reports with cost center owners

Real-World Result:
Better cloud governance and accountability at every level.

81. Software Suites Not Managed as Bundled Licenses

📌 **Clause:** 8.3 – License Tracking

What's Going Wrong:
Software bundles (e.g., Microsoft Office, Adobe Creative Cloud) are tracked as individual components, causing entitlement miscounts.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires accurate license matching. Mismanaging suites inflates deployment data and distorts compliance.

How to Fix It:

✓ Identify bundled software and associate installations under one entitlement

✓ Configure tools to track suite usage collectively

✓ Audit for overcounted or split deployments

Real-World Result:
Better compliance clarity and accurate entitlement usage.

82. Third-Party Tools Are Used Without License Documentation

📌 **Clause:** 8.3.3 – Entitlement Management

What's Going Wrong:
Freeware or open-source tools are installed with no tracking, usage terms, or risk review.

Why It Matters During an Audit:
Lack of documentation on use rights, even for free tools, violates ISO/IEC 19770-1's emphasis on proper entitlement tracking.

How to Fix It:

✓ Maintain a registry of all third-party software with license details

✓ Document usage terms and restrictions

✓ Include freeware in entitlement reviews

Real-World Result:
Improved license transparency and vendor audit readiness.

83. Asset Custody Transfers Not Documented

📌 **Clause:** 8.2.2 – Assignment and Control

What's Going Wrong:
When assets move between departments or users, there's no record of the transfer, causing ownership confusion.

Why It Matters During an Audit:
Audit trails are critical. ISO/IEC 19770-1 expects clear tracking of asset responsibility.

How to Fix It:

✓ Require custody forms or digital sign-offs for each transfer

✓ Update records with new user and location details

✓ Retain logs for lifecycle traceability

Real-World Result:
Reduced asset loss and improved accountability.

84. No ITAM Involvement in New Technology Planning

📌 **Clause:** 6.3 – Planning of Changes

What's Going Wrong:
IT or innovation teams deploy new platforms without consulting asset management, leaving lifecycle and license planning behind.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires involvement in system changes to maintain compliance and control integrity.

How to Fix It:

✓ Include ITAM in IT architecture and procurement review boards

✓ Add lifecycle questions to all change proposals

✓ Flag risks early during planning stages

Real-World Result:
Fewer surprise deployments and improved lifecycle integration.

85. ITAM Policies Are Not Available to End Users

📌 **Clause:** 5.2 – Policy Communication

What's Going Wrong:
Policies exist, but only asset managers have access. Users are unaware of their responsibilities or acceptable use.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates that policies are communicated and understood by all impacted users.

How to Fix It:

✓ Publish policies on the intranet or include them in onboarding

✓ Require acknowledgment or short training for employees

✓ Translate key policies into simplified user guides

Real-World Result:
Greater awareness and reduced unintentional misuse.

86. Devices in Storage Not Counted in Inventory

📌 **Clause:** 8.2.3 – Storage and Idle Assets

What's Going Wrong:
Devices awaiting repair, reuse, or decommissioning are not recorded in the active asset register, creating blind spots.

Why It Matters During an Audit:
All owned assets must be accounted for. Gaps in storage tracking imply missing controls.

How to Fix It:

✓ Include inactive assets in the inventory with “in storage” status

✓ Track physical location, condition, and next steps

✓ Audit storage rooms periodically

Real-World Result:

More accurate inventory and better lifecycle management.

87. Software Not Tagged by Cost Center or Business Unit

📌 **Clause:** 9.1 – Financial Visibility

What’s Going Wrong:

Software purchases are logged centrally, but usage isn’t assigned to departments, limiting cost tracking and budgeting.

Why It Matters During an Audit:

ISO/IEC 19770-1 emphasizes financial responsibility and cost allocation.

How to Fix It:

✓ Tag software with business units, functions, or projects

✓ Track costs and usage by cost center

✓ Share reports with department heads for optimization

Real-World Result:

More informed budgeting and better stakeholder engagement.

88. Assets Deployed with Inconsistent Configuration Standards

📌 **Clause:** 8.2.5 – Configuration Management

What's Going Wrong:
Two identical devices are deployed with different settings, causing inconsistent performance and management overhead.

Why It Matters During an Audit:
Standardization ensures control, supportability, and audit traceability.

How to Fix It:

✓ Apply configuration templates for each asset category

✓ Automate imaging or provisioning processes

✓ Log exceptions and document rationales

Real-World Result:
Lower support effort and greater audit confidence.

89. Renewed Licenses Are Not Tracked Separately

📌 **Clause:** 8.3.3 – License Continuity

What's Going Wrong:
Renewals are lumped with new purchases, making it difficult to track history or reconcile entitlements.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires license lifecycle documentation. Blurred records raise compliance concerns.

How to Fix It:

✓ Record renewals with their original purchase reference

✓ Document effective dates and any term changes

✓ Track renewals in both contract and entitlement logs

Real-World Result:
Improved entitlement auditability and contract alignment.

90. No Integration Between ITAM and Security Incident Response

📌 **Clause:** 6.1 – Risk and Response Planning

What's Going Wrong:
Security teams investigate incidents without access to full asset history, location, or configuration records.

Why It Matters During an Audit:
ISO/IEC 19770-1 promotes integration across governance and risk domains.

How to Fix It:

✓ Share asset metadata with the security incident team

✓ Define joint workflows for incident triage and asset isolation

✓ Update both systems with investigative findings

Real-World Result:
Faster, more informed responses to security breaches and fewer audit gaps.

91. ITAM Program Not Benchmarked Against Industry Best Practices

📌 **Clause:** 10.1 – Improvement

What's Going Wrong:
Performance metrics are reviewed internally but not compared to industry standards or external benchmarks.

Why It Matters During an Audit:
Continuous improvement must be objective. ISO/IEC 19770-1 encourages benchmarking to identify gaps.

How to Fix It:
✓ Use published benchmarks or ISO maturity assessments
✓ Conduct peer comparisons annually
✓ Set improvement targets based on external data

Real-World Result:
Higher system maturity and executive confidence.

92. Cloud Resource Termination Policies Are Undefined

📌 **Clause:** 8.1 / 8.2 – Lifecycle Closure

What's Going Wrong:
Unused cloud instances continue running, accruing costs with no policy for when and how to terminate.

Why It Matters During an Audit:
Lifecycle closure applies to all assets, including virtual ones. Undefined policies reflect immature governance.

How to Fix It:

✓ Set termination criteria (e.g., inactivity thresholds)

✓ Implement scheduled reviews for inactive resources

✓ Include resource tagging and expiry metadata

Real-World Result:

Controlled cloud spend and greater resource accountability.

93. Internal Audit Findings Are Not Shared with Stakeholders

📌 **Clause:** 9.2 – Internal Audit

What's Going Wrong:

Audit reports are filed but not reviewed with IT, procurement, or business owners responsible for actions.

Why It Matters During an Audit:

ISO/IEC 19770-1 expects audit findings to be actionable. Poor communication prevents resolution.

How to Fix It:

✓ Share relevant findings with responsible parties

✓ Assign and track ownership of actions

✓ Close the loop with documented resolutions

Real-World Result:

More effective audits and better cross-functional collaboration.

94. Remote Monitoring Is Not Enabled on Portable Assets

📌 **Clause:** 8.2.4 – Monitoring

What's Going Wrong:
Laptops and mobile devices are frequently unmonitored when offsite, increasing risk of theft or data loss.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes visibility and control, regardless of location.

How to Fix It:
✓ Enable remote tracking and health checks on portable devices
✓ Alert on inactive or offline systems
✓ Require encryption and location reporting

Real-World Result:
Enhanced endpoint security and reduced loss risk.

95. Asset Types Not Prioritized Based on Audit Risk

📌 **Clause:** 6.1 – Risk-Based Focus

What's Going Wrong:
All assets are treated equally in audits, including low-risk or support-only systems.

Why It Matters During an Audit:
Audit focus must reflect asset criticality. Equal coverage wastes resources and weakens impact.

How to Fix It:
✓ Classify assets by audit priority (critical, standard, low-risk)

✓ Adjust frequency and scope based on classification

✓ Reassess priorities yearly

Real-World Result:
More efficient audits and improved resource allocation.

96. No Alerting for Unauthorized Asset Connections

📌 **Clause:** 8.2.4 – Monitoring and Alerting

What's Going Wrong:
Unregistered devices can connect to networks without triggering alerts, risking shadow IT proliferation.

Why It Matters During an Audit:
Auditors look for evidence of real-time controls. Lack of alerting reflects passive governance.

How to Fix It:

✓ Deploy NAC or similar tools to block/alert on unknown devices

✓ Maintain and sync approved asset lists

✓ Review connection logs periodically

Real-World Result:
Reduced exposure to rogue devices and improved network integrity.

97. Software Usage Rights Not Reviewed After Business Model Changes

📌 **Clause:** 8.3.3 – License Validity

What's Going Wrong:
Software licensed for one purpose (e.g., internal use) is repurposed externally after service model changes without entitlement review.

Why It Matters During an Audit:
Licensing terms may no longer apply. ISO/IEC 19770-1 mandates alignment of usage and rights.

How to Fix It:
✓ Review license terms after major service or structural changes
✓ Consult legal or vendor account managers
✓ Adjust entitlements or usage accordingly

Real-World Result:
Avoided vendor penalties and maintained license compliance.

98. No Decommissioning Process for Expired Cloud Licenses

📌 **Clause:** 8.2.6 – Retirement

What's Going Wrong:
Subscriptions lapse or renew by default without review, and assets tied to expired licenses remain active.

Why It Matters During an Audit:
Improper closure violates lifecycle standards. Auditors expect license term governance.

How to Fix It:

✓ Track cloud license expiry and auto-renew dates

✓ Decommission related services and user access

✓ Reallocate or archive assets tied to expired terms

Real-World Result:
Controlled software costs and better user governance.

99. ITAM Audit Trails Are Not Protected from Modification

📌 **Clause:** 7.5 – Record Integrity

What's Going Wrong:
Logs and audit trails can be modified by users without restrictions or traceability.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires integrity of records. Editable logs are not considered credible.

How to Fix It:

✓ Enforce role-based access controls

✓ Use tamper-evident logging systems

✓ Back up logs regularly and archive securely

Real-World Result:
Stronger legal defensibility and audit confidence.

100. Continuous Improvement Plans Are Not Tracked to Completion

📌 **Clause:** 10.1 – Improvement

What’s Going Wrong:
Ideas for improvement are discussed but not documented, tracked, or assigned for follow-up.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires active evidence of continual improvement. Lack of follow-through indicates weak maturity.

How to Fix It:

✓ Log all improvement initiatives with owners and due dates

✓ Review progress in management meetings

✓ Close and archive completed actions with outcomes

Real-World Result:
Stronger program maturity and more consistent audit success.

From Gaps to Governance: Elevating Your ITAM Strategy

Achieving ISO/IEC 19770-1 certification is not simply about passing an audit — it is about embedding a culture of disciplined, transparent, and risk-aware IT Asset Management (ITAM) across your organization.

Throughout this guide, we've outlined 100 of the most common audit non-conformities encountered by experienced ISO/IEC 19770-1 Lead Auditors. These findings span governance, software compliance, lifecycle control, cloud asset oversight, and stakeholder accountability.

Each issue represents not just a missed checklist item, but a potential breakdown in control, efficiency, or trust.

The Key to Success Is Consistency, Visibility, and Control

- **Governance and Accountability:** Clear roles, responsibilities, and policies set the foundation for audit-ready ITAM.
- **Lifecycle Alignment:** From acquisition to retirement — every asset must be tracked, validated, and evaluated.
- **Risk Integration:** ITAM is not a silo — it's a key component of IT security, compliance, and cost management.
- **Evidence-Based Improvement:** Auditors don't just want policies; they want proof of execution and results.

This guide is designed to help you proactively address gaps, strengthen your internal audit capabilities, and align your ITAM strategy with the expectations of the ISO/IEC 19770-1 framework.

GSDC
Global Skill Development Council

CERTIFIED ISO/IEC 19770 1 LEAD AUDITOR

A Certified ISO 19770-1 Lead Auditor is based on IT asset management audits.

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

- **Develop a deep understanding of the concepts and practical application of ISO 19770-1:2017 Lead Auditor Training.**
- **Identify the necessary documentation as per ISO 19770-1:2017 standards.**
- **Familiarize yourself with the procedure and resource requirements involved.**
- **Master the use of audit checklists and internal auditing.**

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

Enroll Now

✉ www.gsdcouncil.org