ISO/IEC 19770-1 Lead Auditor Guide: Tackling the Top 100 Non-Conformities

A comprehensive roadmap for identifying, addressing, and fixing common audit failures to ensure successful ISO/IEC 19770-1 certification and compliance.

Introduction

ISO/IEC 19770-1 provides a comprehensive framework for IT Asset Management (ITAM), emphasizing the importance of managing IT assets efficiently and securely. Achieving ISO/IEC 19770-1 certification is crucial for organizations looking to optimize asset management processes, mitigate risks, and ensure compliance with industry standards.

However, during audits, organizations often face common non-conformities that can lead to delays in certification or additional costs. These non-conformities, if not addressed, can significantly hinder the progress of an organization's ITAM initiatives.

This document outlines 100 of the most common audit failures organizations encounter during an ISO/IEC 19770-1 audit. For each failure, we provide insightful solutions based on best practices, ensuring that your organization can close the gaps and align with ISO/IEC 19770-1 requirements effectively.

Objectives of This Guide

- **Identify common non-conformities** organizations face during ISO/IEC 19770-1 audits.
- Provide **practical solutions** to address and rectify non-conformities.
- **Increase compliance readiness** by aligning your asset management practices with ISO/IEC 19770-1 standards.
- Enable continuous **improvement of ITAM processes** to support future audits and certifications.
- Help your organization achieve and maintain **ISO/IEC 19770-1 certification** with confidence.

Who Should Use This Guide?

- **ISO/IEC 19770-1 Lead Auditors** looking to prepare for certification audits or internal reviews.
- **IT Asset Managers and Compliance Teams** striving for ISO/IEC 19770-1 certification or looking to improve asset management processes.
- **CIOs, CTOs, and Procurement Teams** who are responsible for managing IT assets and aligning them with regulatory and compliance frameworks.
- **IT Consultants and Advisors** helping organizations navigate the ISO/IEC 19770-1 certification process.

How to Use This Guide

This guide is divided into **10 sections**, each focusing on a specific category of common non-conformities related to **ISO/IEC 19770-1**. For each non-conformity, the following format is used:

- **Clause:** The specific clause from ISO/IEC 19770-1 that the non-conformity pertains to.
- **What's Going Wrong:** A description of the common issue organizations face related to the non-conformity.
- **Why It Matters During an Audit:** Explanation of why this non-conformity can impact your audit and certification process.
- **How to Fix It:** Actionable solutions that can be implemented to address the non-conformity and ensure compliance.
- **Real-World Result:** A tangible outcome that results from addressing the non-conformity.

1. No Formal IT Asset Management Policy

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

What's Going Wrong:
Many organizations do not have a formal, documented policy for IT Asset Management (ITAM). This leads to inconsistent processes and unclear governance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a documented ITAM policy to ensure a structured approach to asset management. Auditors expect to see clear leadership commitment and alignment with organizational objectives.

How to Fix It:
✓ Develop and document a formal ITAM policy that includes asset identification, procurement, and disposal procedures.
✓ Align the policy with organizational goals and ensure it is endorsed by top management.
✓ Regularly review and update the policy to adapt to changes in the business environment.

Real-World Result:
A formal ITAM policy establishes clear roles and processes, improving compliance and creating a foundation for ongoing improvements.

2. Incomplete or Outdated Asset Inventory

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

What's Going Wrong:
Asset inventories are often incomplete or outdated, leading to discrepancies between the actual assets and what's recorded in the system.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires organizations to maintain an accurate and up-to-date asset inventory. Inaccurate records can lead to financial misreporting and compliance issues.

How to Fix It:
✓ Implement an automated asset discovery tool to track assets in real-time.
✓ Regularly update the asset register and reconcile it with physical assets.
✓ Assign ownership for asset records and review inventory accuracy quarterly.

Real-World Result:
An accurate asset inventory improves compliance with ISO/IEC 19770-1, enhances asset traceability, and reduces audit risks.

3. No Clear Roles and Responsibilities for ITAM

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

What's Going Wrong:
Roles and responsibilities for IT Asset Management (ITAM) are often not well-defined, resulting in confusion about who is accountable for asset tracking and compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires clear documentation of roles and responsibilities for asset management to ensure accountability. Lack of clarity can result in audit discrepancies and inefficiencies.

How to Fix It:

✓ Define and document roles for each stage of the asset lifecycle (e.g., procurement, asset tracking, disposal).

✓ Use a **RACI matrix** (Responsible, Accountable, Consulted, and Informed) to clarify ownership of ITAM tasks.

✓ Ensure all employees involved in ITAM activities are trained on their responsibilities.

Real-World Result:

Clear role definition improves communication, reduces errors, and helps ensure compliance during audits.

4. Uncontrolled Software License Usage

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

What's Going Wrong:

Software licenses are not tracked or monitored properly, leading to overuse, underuse, or non-compliance with licensing agreements.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires organizations to have a controlled approach to software license management. Failure to track software usage increases the risk of compliance violations and penalties.

How to Fix It:

✓ Implement software license metering tools to track usage.

✓ Regularly reconcile software installations with license entitlements.

✓ Establish a process for software procurement and distribution to ensure compliance from the outset.

Real-World Result:
Better software license compliance, optimized costs, and reduced risk of vendor audits and penalties.

5. Inadequate Risk Management for IT Assets

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

What's Going Wrong:
Risk management for IT assets is either informal or not documented, leading to unaddressed vulnerabilities and inefficiencies.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes the need for risk management to ensure that assets are safeguarded against threats, such as unauthorized access, theft, or damage.

How to Fix It:
✓ Identify and assess risks associated with IT assets (e.g., data loss, software piracy).
✓ Implement risk mitigation measures and assign responsible parties for managing risks.
✓ Review and update risk management procedures regularly.

Real-World Result:
A proactive risk management approach reduces vulnerabilities, increases asset protection, and strengthens overall compliance.

6. No Clear Process for Software and Hardware Disposal

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

What's Going Wrong:
Disposal processes for hardware and software are either non-existent or poorly defined, leading to potential data security breaches or environmental compliance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a secure and documented process for asset disposal. Failure to properly manage asset disposal could result in data breaches or environmental fines.

How to Fix It:
✓ Develop a formal asset disposal policy, including secure data destruction practices.
✓ Use certified e-waste recycling vendors for disposal and obtain certificates of destruction.
✓ Ensure that assets are tracked until the disposal process is completed.

Real-World Result:
Secure disposal practices mitigate data risks, ensure environmental compliance, and strengthen the organization's reputation.

7. No Regular Internal Audits of ITAM Processes

📌 **Clause:** 9.2 – Internal Audit

What's Going Wrong:
Internal audits of ITAM processes are infrequent or not performed, making it difficult to identify gaps or inefficiencies in asset management practices.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates regular internal audits to assess the effectiveness of the ITAM system and ensure continuous improvement.

How to Fix It:
✓ Schedule regular internal audits of ITAM processes to identify non-conformities.
✓ Use internal audits as an opportunity to refine policies and procedures.
✓ Track audit findings and corrective actions to ensure continual improvement.

Real-World Result:
Proactive audits help catch non-conformities early and enhance compliance over time.

8. Lack of User Training on Asset Management Policies

📌 **Clause:** 7.3 – Awareness

What's Going Wrong:
Employees are not trained on ITAM policies, leading to inconsistent handling of assets, from procurement to disposal.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires awareness and competency across the organization to ensure that ITAM policies are followed correctly.

How to Fix It:
✓ Provide regular ITAM training to all relevant stakeholders.
✓ Include ITAM policy education in the onboarding process for new employees.
✓ Conduct periodic refresher courses to reinforce best practices.

Real-World Result:
Employee awareness improves adherence to ITAM processes, reducing errors and strengthening compliance.

9. No Defined Software Reallocation Process

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

What's Going Wrong:
When employees leave or change roles, software licenses are not properly reallocated or reassigned, leading to wasted entitlements.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes the need for effective license management. Failing to reallocate unused licenses results in unnecessary costs and audit discrepancies.

How to Fix It:
✓ Implement a formal process to track software license reallocation.
✓ Use an automated tool to check for unused or underused licenses.
✓ Ensure that all software licenses are reassigned or decommissioned during employee offboarding.

Real-World Result:
Better software cost management, improved compliance, and optimized license usage.

10. No Asset Recovery Process for Leased Equipment

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

What's Going Wrong:
Leased equipment, such as laptops or servers, is not tracked for timely return at the end of the leasing period, leading to asset losses or untracked liabilities.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that leased assets be included in the asset management system and properly tracked through their lifecycle. Failure to do so could result in untracked costs and missing assets.

How to Fix It:
✓ Implement a process to track leased assets, including due return dates.
✓ Include asset recovery as part of the offboarding process for employees.
✓ Regularly review lease agreements and ensure timely return of leased equipment.

Real-World Result:
Reduced costs, improved asset control, and stronger vendor relations.

11. No Clear Process for Handling Orphaned or Unused Software

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

What's Going Wrong:
Unused or orphaned software (software that is not associated with a user or business unit) is not properly tracked or removed from the system, leading to waste.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes software lifecycle management. Unused software can lead to unnecessary costs, security risks, and compliance gaps.

How to Fix It:
✓ Periodically audit software usage to identify and remove unused or

orphaned software.

✓ Implement a software usage monitoring tool that can flag unused applications.

✓ Create a policy for the proper disposal or reassignment of unused software.

Real-World Result:
Lower software costs, improved license compliance, and reduced operational risk.

12. No Record of Asset Ownership Changes

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
When assets are transferred between departments or owners, the changes are not documented, leading to confusion and accountability issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires clear documentation of asset ownership for effective tracking and compliance.

How to Fix It:

✓ Implement an asset transfer log for all movements of assets between departments or users.

✓ Use asset management software to track ownership changes and assign responsibilities.

✓ Review asset ownership records during routine audits to ensure they are up to date.

Real-World Result:
Improved asset tracking, better accountability, and smoother audits.

13. No Integration Between ITAM and Change Management Processes

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

What's Going Wrong:
Changes to IT infrastructure or assets (e.g., upgrades, reconfigurations) are made without updating the ITAM system, leading to discrepancies in asset records.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires the integration of asset management processes with change management to maintain accurate records and prevent asset mismanagement.

How to Fix It:
✓ Ensure that all asset changes are logged in the ITAM system.
✓ Integrate ITAM with change management tools to automatically update asset records.
✓ Train teams to follow a standardized process for reporting changes to IT assets.

Real-World Result:
Improved asset visibility, more accurate records, and streamlined change management.

14. Lack of Asset Lifecycle Control for Cloud Assets

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

What's Going Wrong:
Cloud-based assets are not treated with the same rigor as physical assets.

There is no clear lifecycle process for provisioning, monitoring, and decommissioning cloud resources.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, including virtual and cloud-based resources, be fully managed through their lifecycle. This ensures better control and compliance.

How to Fix It:
✓ Implement lifecycle management processes for cloud-based assets.
✓ Use cloud management tools to track resource usage and decommissioning.
✓ Establish protocols for the procurement, assignment, and retirement of cloud assets.

Real-World Result:
Better cloud asset management, improved compliance, and optimized cloud spending.

15. Inadequate Controls for Unmanaged IT Assets

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Some assets, such as those brought in by employees (BYOD) or those provisioned by departments outside of IT, are not included in the asset management system.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires comprehensive tracking of all assets. Unmanaged assets pose security risks and can lead to compliance failures.

How to Fix It:
✓ Implement policies for tracking and managing all devices, including

BYOD.

✓ Use automated tools to detect and manage unmanaged assets.

✓ Include all assets in the asset inventory, regardless of how they were procured.

Real-World Result:
Improved asset control and reduced risk from unmanaged devices.

16. No Defined Process for Software License Procurement

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

What's Going Wrong:
Software is procured without a standardized process, leading to inconsistent licensing agreements, missed renewals, and overspending.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a standardized approach to software procurement to ensure that software usage is compliant with licensing agreements.

How to Fix It:

✓ Establish a formal procurement process for all software purchases.

✓ Ensure that all software licenses are reviewed by ITAM before purchase.

✓ Track software renewals and updates through automated reminders.

Real-World Result:
Optimized software procurement, reduced costs, and ensured license compliance.

17. No Documentation for Asset Disposal Process

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

What's Going Wrong:
Assets are disposed of without documentation, leading to data security risks and non-compliance with regulatory requirements.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, including retired or disposed assets, be handled securely and in compliance with data protection regulations.

How to Fix It:
✓ Create a formal asset disposal process that includes secure data destruction.
✓ Use certified disposal vendors and retain certificates of destruction.
✓ Document the entire disposal process, including asset details and disposal dates.

Real-World Result:
Reduced risk of data breaches and compliance violations.

18. No Software Reconciliation After System Upgrades

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

What's Going Wrong:
Software installations are not reconciled after system upgrades or changes, leading to mismatches between licensed software and actual installations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires regular software reconciliation to ensure that license usage matches the organization's entitlements.

How to Fix It:
✓ Implement a process for reconciling software licenses after system upgrades or changes.
✓ Use software management tools to track installations and compare them with license records.
✓ Conduct regular audits to verify software compliance after major changes.

Real-World Result:
Better software compliance, fewer audit issues, and optimized software usage.

19. No Periodic Review of IT Asset Management Policies

📌 **Clause:** 5.3 – Review of Policies

What's Going Wrong:
ITAM policies are developed but not regularly reviewed or updated to reflect changes in technology, business needs, or regulatory requirements.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that ITAM policies be regularly reviewed and updated to stay relevant and effective.

How to Fix It:
✓ Schedule annual reviews of ITAM policies to ensure they remain aligned with business goals.
✓ Involve key stakeholders in policy reviews to gather feedback.
✓ Update policies as necessary to address emerging risks or opportunities.

Real-World Result:
Stronger, more adaptable policies and improved audit readiness.

20. No Clear Methodology for Software Entitlement Tracking

📌 **Clause:** 8.3.3 – License Management

What's Going Wrong:
Software entitlements are not tracked consistently or clearly, leading to uncertainty over which licenses are available for deployment.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a clear methodology for tracking and managing software entitlements to ensure compliance.

How to Fix It:
✓ Establish a standardized method for tracking software entitlements.
✓ Use automated tools to ensure real-time visibility of license availability.
✓ Regularly reconcile entitlements with actual software deployments.

Real-World Result:
Better visibility, reduced license over-purchase, and enhanced audit accuracy.

21. No Process for Managing IT Asset Lifecycle for Cloud Resources

📌 **Clause:** 8.1 – Asset Identification and Lifecycle Management

What's Going Wrong:
Cloud assets are treated informally and often fall outside the formal ITAM lifecycle, creating gaps in tracking and usage.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires all assets, including cloud-based resources, to be managed throughout their lifecycle. Lack of control over cloud assets can lead to financial and security risks.

How to Fix It:

✓ Define a clear lifecycle management process for cloud resources.

✓ Include cloud assets in the asset register and ensure they are tracked from procurement to decommissioning.

✓ Use cloud management tools to monitor usage and cost.

Real-World Result:
Improved cloud asset visibility and cost management, with reduced risk from untracked resources.

22. No Process for Tracking and Managing Software in Virtual Environments

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

What's Going Wrong:
Software used in virtual environments is not tracked or managed separately, leading to over-usage or unmonitored deployments.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires software licenses to be fully tracked, including those used in virtual environments. Without proper management, there's a risk of non-compliance.

How to Fix It:

✓ Implement tools to track software usage in virtual environments.

✓ Include virtual machines and containers in the asset inventory.

✓ Regularly reconcile software deployments with license entitlements.

Real-World Result:
Enhanced control over virtual environments, ensuring compliance and cost optimization.

23. No Centralized System for Asset Registration

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Assets are registered in multiple, disconnected systems, leading to inconsistencies and difficulty in accessing comprehensive asset data.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects a centralized system to provide a single source of truth for all asset data. Dispersed records create inefficiencies and confusion during audits.

How to Fix It:
✓ Implement a centralized ITAM system that integrates with other enterprise tools.
✓ Ensure all asset-related data (e.g., hardware, software, licenses) is entered and updated in the central system.
✓ Periodically audit and reconcile data between systems to maintain consistency.

Real-World Result:
Improved asset tracking and reporting, with greater efficiency during audits.

24. No Clear Guidelines for Asset Procurement and Acquisition

📌 **Clause:** 8.2 – Procurement and Acquisition

What's Going Wrong:
Asset procurement is carried out without standardized processes, leading to inconsistent tracking and non-compliance with asset management policies.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a documented, standardized process for asset procurement to ensure proper tracking and compliance from the outset.

How to Fix It:
✓ Define a formal procurement process that includes ITAM and compliance checks.
✓ Use procurement software that integrates with the ITAM system for real-time asset tracking.
✓ Establish clear guidelines for hardware, software, and cloud service acquisitions.

Real-World Result:
Streamlined procurement processes, ensuring compliance and preventing over-purchasing or non-compliant acquisitions.

25. Assets Are Not Categorized by Criticality

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

What's Going Wrong:
Assets are not categorized based on their criticality or importance to the organization, leading to inconsistent management and oversight.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes the need for a risk-based approach to asset management. Assets should be categorized by criticality to ensure appropriate controls.

How to Fix It:
✓ Create a categorization system for assets based on their risk, value, and criticality.
✓ Implement controls tailored to each category (e.g., higher security for critical assets).
✓ Review and update asset categories annually to reflect changing business needs.

Real-World Result:
Prioritized asset management and improved risk mitigation, especially for critical resources.

26. No Continuous Improvement Plan for ITAM Processes

📌 **Clause:** 10.1 – Improvement

What's Going Wrong:
ITAM processes are static and not regularly reviewed for potential improvements, leading to inefficiencies or non-compliance over time.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires continuous improvement of the ITAM system to ensure it remains effective and aligned with organizational needs.

How to Fix It:
✓ Establish a formal process for reviewing and improving ITAM practices.
✓ Set performance indicators for ITAM processes and measure them regularly.

✓ Include feedback from internal audits, user input, and industry best practices in your improvement plan.

Real-World Result:
Ongoing process optimization, leading to improved efficiency, compliance, and cost-effectiveness.

27. Insufficient Documentation for ITAM Policies and Procedures

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
ITAM policies and procedures are either not documented or not sufficiently detailed, making it difficult to ensure compliance and effective execution.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that policies, procedures, and other key information be well-documented and easily accessible to relevant stakeholders.

How to Fix It:
✓ Document all ITAM policies, procedures, and controls.
✓ Ensure that policies are easily accessible to stakeholders across the organization.
✓ Review and update documentation regularly to ensure relevance and completeness.

Real-World Result:
Clear, accessible documentation leads to better policy compliance, fewer audit issues, and greater organizational alignment.

28. Lack of Compliance with Data Privacy Regulations

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

What's Going Wrong:
IT assets, especially those with sensitive data, are not disposed of according to data privacy regulations, leading to potential data breaches and non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, especially those containing sensitive information, be handled and disposed of in accordance with privacy regulations, such as GDPR or HIPAA.

How to Fix It:
✓ Develop and implement a data disposal policy that complies with relevant data privacy regulations.
✓ Use certified data destruction services for hard drives, storage devices, and sensitive assets.
✓ Document all asset disposal activities and retain certificates of destruction.

Real-World Result:
Better data protection, compliance with data privacy laws, and reduced risk of data breaches.

29. Lack of a Clear Asset Reconciliation Process After System Changes

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

What's Going Wrong:
After significant system changes (e.g., upgrades, migrations), assets are not

reconciled with the updated system, leading to discrepancies in asset records.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires asset records to be accurate and up-to-date. Failure to reconcile assets after system changes can result in inaccuracies and non-compliance.

How to Fix It:
✓ Establish a formal process for asset reconciliation after any major system changes.
✓ Use asset management software that integrates with IT systems to ensure data consistency.
✓ Conduct regular reviews to ensure that the asset register is always up-to-date.

Real-World Result:
Accurate asset records, better change management, and improved audit preparedness.

30. No Integration Between ITAM and Security Management Systems

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

What's Going Wrong:
Asset management and security systems operate independently, creating gaps in security visibility and control over IT assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires integration with security systems to ensure that assets are properly protected, monitored, and managed throughout their lifecycle.

How to Fix It:

✓ Integrate your ITAM system with security tools for real-time monitoring and alerts.

✓ Ensure that all assets are included in both asset management and security systems.

✓ Regularly audit security policies and asset access controls.

Real-World Result:

Improved asset security and better compliance with organizational security standards.

31. No Formal Software License Review Process

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

What's Going Wrong:

Software licenses are not reviewed regularly, leading to discrepancies in license usage and potential over-usage or under-usage of software.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires periodic review of software licenses to ensure compliance with terms and conditions.

How to Fix It:

✓ Establish a routine software license review process.

✓ Conduct regular audits to compare installed software with license entitlements.

✓ Implement automated license tracking tools to monitor usage.

Real-World Result:

More efficient license usage, reduced risk of software non-compliance, and better audit preparedness.

32. No Clear Ownership for Software License Management

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

What's Going Wrong:
There is no designated individual or team responsible for software license management, leading to oversight and non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires clear ownership and accountability for software license management to ensure compliance and reduce risks.

How to Fix It:
✓ Assign a dedicated team or individual to oversee software license management.
✓ Establish clear roles and responsibilities for procurement, tracking, and compliance.
✓ Ensure regular training and support for those managing software licenses.

Real-World Result:
Improved compliance and accountability in software license management, with fewer audit discrepancies.

33. No Formal Process for Asset Depreciation and Disposal

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

What's Going Wrong:
Assets are not formally depreciated or disposed of according to their lifecycle, leading to excess assets or untracked depreciations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires assets to be properly depreciated and retired according to established schedules. Non-compliance leads to audit discrepancies.

How to Fix It:
✓ Implement a clear asset depreciation and retirement policy.
✓ Set depreciation schedules based on asset type and usage.
✓ Ensure proper documentation of asset disposal and retirement.

Real-World Result:
Improved financial accuracy, reduced asset waste, and enhanced audit processes.

34. No Formal Control Over Temporary or Spare Assets

📌 **Clause:** 8.2.4 – Asset Control

What's Going Wrong:
Temporary or spare assets, such as backup hardware or spare software licenses, are not formally tracked or controlled, leading to potential misuse or loss.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, even temporary ones, be tracked and controlled to ensure compliance and effective asset management.

How to Fix It:
✓ Implement a process to track all temporary or spare assets, including storage and usage.
✓ Assign unique identifiers to spare assets and monitor their usage.
✓ Periodically review spare assets to ensure they are appropriately managed.

Real-World Result:
Improved control over spare resources and better asset visibility.

35. Inadequate Security for IT Assets

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

What's Going Wrong:
There are insufficient security measures for IT assets, especially those containing sensitive data or critical infrastructure.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates that appropriate security measures be implemented for IT assets to mitigate risks of data breaches or loss.

How to Fix It:
✓ Implement strong access controls for IT assets, especially those containing sensitive data.
✓ Regularly audit and monitor asset access to identify potential security vulnerabilities.
✓ Ensure that all assets are encrypted and securely stored.

Real-World Result:
Improved data protection and reduced risk of security incidents or breaches.

36. Incomplete or Poorly Managed Asset Documentation

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
Asset documentation is incomplete or lacks detail, making it difficult to manage assets and ensure compliance with ISO/IEC 19770-1.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT asset documentation be thorough, accurate, and up-to-date to ensure compliance.

How to Fix It:
✓ Ensure that all asset documentation includes essential details (e.g., purchase date, software version, licensing).
✓ Implement a standardized format for documenting assets across all departments.
✓ Regularly review and update asset records to maintain accuracy.

Real-World Result:
Improved asset traceability and easier compliance verification during audits.

37. No Formal Process for Asset Recovery After Employee Termination

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

What's Going Wrong:
When employees leave the organization, assets are not consistently recovered or reassigned, leading to missing equipment or unauthorized asset use.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that assets be recovered, reassigned, or securely disposed of when employees leave to maintain control and reduce risk.

How to Fix It:
✓ Integrate asset recovery into the employee offboarding process.

✓ Maintain a checklist for all assets that need to be recovered during offboarding.
✓ Track all recovered assets and update the ITAM system immediately.

Real-World Result:
Better asset recovery, reduced asset loss, and increased security.

38. No Automated Alerts for Software License Expirations

📌 **Clause:** 8.3.3 – License Management

What's Going Wrong:
Software license expirations are not tracked automatically, leading to missed renewals and potential service disruptions or non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires proactive management of software licenses to avoid lapses. Missed renewals can result in compliance issues.

How to Fix It:
✓ Implement automated alerts for upcoming software license expirations.
✓ Set reminders for renewals and re-evaluations of software entitlements.
✓ Track software license terms and expiry dates in a centralized system.

Real-World Result:
Improved license compliance and uninterrupted software usage.

39. No Asset Classification System

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Assets are not classified according to their value, function, or criticality, leading to inefficient management and oversight.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires asset classification to ensure that high-value or critical assets receive more robust controls and oversight.

How to Fix It:
✓ Develop an asset classification system based on factors such as value, criticality, and security needs.
✓ Ensure that high-priority assets are tracked more rigorously, with additional controls.
✓ Regularly review asset classification to ensure it reflects business priorities.

Real-World Result:
Improved management of critical assets and more efficient use of resources.

40. No Asset Tagging for Physical Assets

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Physical assets (e.g., computers, servers) are not tagged or labeled with unique identifiers, making it difficult to track them effectively.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, especially physical ones, be clearly identifiable for tracking, management, and security purposes.

How to Fix It:
✓ Implement a system for tagging all physical assets with unique identifiers (e.g., barcodes, RFID).
✓ Ensure that asset tags are durable and can withstand the asset's environment.
✓ Regularly scan and update asset information based on tag data.

Real-World Result:
Enhanced asset tracking and improved security, with easier reconciliation during audits.

41. No Clear Ownership for Software License Compliance

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

What's Going Wrong:
There is no clearly defined individual or team responsible for ensuring software license compliance, leading to inconsistencies and potential overuse of licenses.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that software license compliance be assigned to a specific individual or team to ensure accountability and prevent violations.

How to Fix It:
✓ Assign a dedicated team or individual to manage software licenses and compliance.
✓ Document roles and responsibilities for license management and ensure

ongoing training.

✓ Conduct regular reviews of software license agreements and usage.

Real-World Result:
Better control over software licenses, optimized costs, and a more efficient audit process.

42. Inconsistent Asset Verification Processes

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

What's Going Wrong:
There is no consistent or formal process for verifying the accuracy of asset records, leading to discrepancies and errors in asset management.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires regular asset verification to ensure the accuracy of asset records. Inconsistent verification practices increase the likelihood of errors and non-compliance.

How to Fix It:

✓ Establish a regular asset verification schedule (e.g., annual or quarterly).

✓ Perform physical audits to reconcile actual assets with records in the ITAM system.

✓ Implement automated tools to monitor asset status and flag discrepancies.

Real-World Result:
Improved asset accuracy, better control over physical assets, and smoother audit processes.

43. No Formal Process for Managing Cloud Service Contracts

📌 **Clause:** 8.2.6 – Contract Management

What's Going Wrong:
Cloud service contracts are not managed centrally, leading to missed renewal dates, duplicate services, or compliance gaps.

Why It Matters During an Audit:
ISO/IEC 19770-1 expects comprehensive management of all asset contracts, including cloud services. Without proper contract management, your organization may face unnecessary expenses or compliance violations.

How to Fix It:
✓ Create a centralized system for tracking all cloud service contracts, including terms, renewals, and service-level agreements (SLAs).
✓ Set up automated alerts for contract renewals or review periods.
✓ Ensure contracts are reviewed regularly to confirm compliance with service terms.

Real-World Result:
Better management of cloud services, improved cost control, and ensured compliance with contract terms.

44. No Process for Tracking Asset Usage Across Different Locations

📌 **Clause:** 8.2.4 – Asset Tracking and Control

What's Going Wrong:
Assets that are deployed across multiple locations are not tracked consistently, leading to confusion and potential loss of assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, regardless of location, be tracked and managed effectively to ensure visibility and accountability.

How to Fix It:
✓ Implement a location-based asset tracking system that records the physical location of each asset.
✓ Use asset tracking tools like RFID or barcode scanning to monitor assets in real-time.
✓ Ensure regular reconciliation of assets at each location.

Real-World Result:
Improved asset control and visibility across all locations, making audits smoother and more accurate.

45. Lack of ITAM Process for Mergers and Acquisitions

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

What's Going Wrong:
During mergers or acquisitions, there is no clear process for integrating IT asset management systems, leading to discrepancies in asset ownership and license compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that asset management systems remain consistent and compliant, even during organizational changes. Failure to integrate systems properly can lead to non-compliance and missed opportunities for optimization.

How to Fix It:
✓ Create a formal ITAM integration process for mergers and acquisitions.
✓ Reconcile asset inventories and software licenses post-merger.

✓ Review and update asset management policies to reflect the combined organization's needs.

Real-World Result:
A seamless integration of IT asset management during mergers, ensuring compliance and reducing operational disruption.

46. No Process for Managing IT Asset Transfers Across Business Units

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

What's Going Wrong:
IT assets transferred between business units or departments are not tracked, leading to a lack of visibility and accountability.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all asset transfers be documented and tracked to ensure compliance with asset management processes.

How to Fix It:
✓ Implement a formal process for documenting and tracking asset transfers.
✓ Use asset management software to record changes in ownership and location.
✓ Conduct periodic reviews to ensure asset transfers are properly recorded and completed.

Real-World Result:
Better visibility of asset movement, improved accountability, and fewer discrepancies during audits.

47. Lack of Integration Between ITAM and Financial Systems

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
IT asset management and financial systems are not integrated, leading to misalignment between financial records and asset inventories.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires financial tracking and IT asset management to be closely aligned. Discrepancies can result in inaccurate financial reporting and audit complications.

How to Fix It:
✓ Integrate ITAM systems with financial systems to ensure consistency in asset valuations and costs.
✓ Track asset depreciation and capital expenditures alongside asset records.
✓ Regularly reconcile financial and asset records for accuracy.

Real-World Result:
Improved financial accuracy, more efficient resource allocation, and streamlined audit processes.

48. Failure to Identify and Mitigate Risks Related to Third-Party Software

📌 **Clause:** 6.1 – Risk Management

What's Going Wrong:
Organizations fail to assess and mitigate risks associated with third-party software, including security vulnerabilities and compliance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires organizations to identify and manage risks related to IT assets, including third-party software. Failure to do so can expose the organization to security breaches and legal liabilities.

How to Fix It:
✓ Regularly assess third-party software for compliance and security risks.
✓ Develop a process for reviewing and approving third-party software before installation.
✓ Implement security controls for third-party software to mitigate risks.

Real-World Result:
Reduced security risks and better compliance with third-party software agreements.

49. No Visibility or Control Over Shadow IT

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Employees or departments purchase and deploy their own IT assets without informing IT or asset management, leading to uncontrolled and untracked devices.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT assets, regardless of how they are acquired, be tracked and controlled. Shadow IT poses risks to security and compliance.

How to Fix It:
✓ Implement a process for registering and monitoring all IT assets, regardless of how they are procured.
✓ Educate employees about the importance of reporting any IT assets they

use.

✓ Use automated discovery tools to detect unauthorized devices on the network.

Real-World Result:
Improved asset visibility, enhanced security, and reduced risks from unauthorized IT assets.

50. No Data Analytics for ITAM Performance and Compliance

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

What's Going Wrong:
ITAM performance is not tracked using data analytics, leading to missed opportunities for improvement and a lack of insight into compliance gaps.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires ongoing monitoring and measurement of ITAM processes to ensure continuous improvement and compliance.

How to Fix It:

✓ Implement analytics tools to track ITAM performance against key metrics.

✓ Regularly review performance data and use it to refine processes.

✓ Use data to identify areas of risk or non-compliance and address them proactively.

Real-World Result:
Better decision-making, enhanced performance, and improved compliance outcomes.

51. Lack of Proper Software Entitlement Tracking

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

What's Going Wrong:
Software entitlements are not adequately tracked, leading to issues with license usage and compliance during audits.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires organizations to have a clear system for tracking software entitlements to ensure that license usage matches the organization's actual needs.

How to Fix It:
✓ Implement a software entitlement management system to track license terms, limits, and usage.
✓ Perform regular reconciliations between entitlements and deployments.
✓ Set up automated alerts for underused or overused licenses.

Real-World Result:
Improved software compliance, optimized license usage, and fewer discrepancies during audits.

52. No Control Over Temporary or Borrowed IT Assets

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

What's Going Wrong:
Temporary or borrowed IT assets, such as loaner devices or project-specific equipment, are not tracked, leading to unaccounted assets and potential losses.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates control over all IT assets, regardless of their status (temporary or borrowed). Without proper tracking, assets can be lost or misused.

How to Fix It:
✓ Implement a process for registering and tracking temporary or borrowed assets.
✓ Use asset tags and require sign-in/sign-out procedures for temporary assets.
✓ Regularly review the status of temporary assets and ensure they are returned or reassigned.

Real-World Result:
Better control over temporary resources and fewer instances of missing or untracked assets.

53. No Automated Tools for License Compliance Audits

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

What's Going Wrong:
License compliance is managed manually, making it difficult to track and report accurately, especially with large numbers of software assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes automation in managing license compliance, as manual processes are prone to error and inefficiency during audits.

How to Fix It:
✓ Implement automated license compliance tools that track usage and entitlements in real-time.
✓ Use reporting features to automatically generate license compliance

reports for audits.

✓ Integrate automated tools with your ITAM system to ensure seamless data synchronization.

Real-World Result:
Faster audits, reduced errors, and more accurate license compliance tracking.

54. Untracked Cloud Resource Usage

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

What's Going Wrong:
Cloud resources such as computing power, storage, and services are used without being tracked, leading to unoptimized costs and non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT assets, including cloud resources, be tracked and managed. Failing to do so can lead to overspending and poor visibility.

How to Fix It:

✓ Implement cloud resource management tools to monitor and track cloud usage.

✓ Tag and categorize cloud resources by department, project, or cost center.

✓ Review cloud resources regularly to ensure usage aligns with organizational needs.

Real-World Result:
Improved cloud cost optimization and better alignment of cloud resources with business priorities.

55. Insufficient Reporting on IT Asset Utilization

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

What's Going Wrong:
There are no clear metrics or reports available on asset utilization, making it difficult to assess whether assets are being used efficiently.

Why It Matters During an Audit:
ISO/IEC 19770-1 stresses the need for ongoing monitoring and measurement of asset performance to ensure that assets are being utilized effectively and compliantly.

How to Fix It:
✓ Implement asset utilization tracking tools to monitor how and when assets are being used.
✓ Establish key performance indicators (KPIs) for asset utilization.
✓ Regularly review and optimize the use of underused assets to maximize ROI.

Real-World Result:
Better asset utilization, improved financial control, and reduced waste.

56. Lack of Regular Software Inventory Audits

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

What's Going Wrong:
Software inventories are not audited regularly, leading to discrepancies between installed software and recorded licenses.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that software inventories be periodically

reviewed and reconciled to ensure compliance and avoid licensing violations.

How to Fix It:

✓ Schedule regular software inventory audits (e.g., annually or quarterly).

✓ Use automated software inventory tools to streamline audits and track installations.

✓ Reconcile software licenses with actual installations and usage during each audit.

Real-World Result:

Improved software license compliance, reduced risk of over-deployment, and streamlined audit processes.

57. No Defined Process for Hardware Lifecycle Management

📌 **Clause:** 8.2 – Lifecycle Management

What's Going Wrong:

There is no formal process for managing the lifecycle of hardware assets, leading to inefficiencies, missed opportunities for optimization, and non-compliance.

Why It Matters During an Audit:

ISO/IEC 19770-1 mandates a structured process for managing hardware assets throughout their lifecycle, from procurement to retirement, to ensure compliance.

How to Fix It:

✓ Define and document processes for hardware asset acquisition, tracking, maintenance, and disposal.

✓ Ensure regular audits of hardware assets to track their condition and compliance.

✓ Track hardware depreciation and allocate resources based on lifecycle stage.

Real-World Result:
Better control of hardware assets, improved lifecycle management, and reduced audit discrepancies.

58. No Defined Policy for IT Asset Borrowing

📌 **Clause:** 8.2.2 – Asset Control

What's Going Wrong:
Employees borrow IT assets without any formal procedure, leading to potential asset loss and a lack of tracking.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, including those temporarily borrowed by employees, be properly tracked and controlled to ensure accountability.

How to Fix It:
✓ Implement a formal asset borrowing policy that includes asset logging and approval procedures.
✓ Use asset management software to track borrowed items and their return dates.
✓ Ensure that employees are trained on the borrowing process and responsibilities.

Real-World Result:
Improved asset control, reduced loss risk, and smoother audit processes.

59. No Visibility Into External IT Assets (e.g., Third-Party Equipment)

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Third-party IT assets, such as vendor equipment or leased devices, are not tracked, creating gaps in asset management and increasing audit risk.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, whether owned or external, be tracked and managed to maintain control and ensure compliance.

How to Fix It:
✓ Ensure all third-party IT assets are included in the asset inventory and tracked in the ITAM system.
✓ Establish processes for monitoring and reporting on third-party asset usage and compliance.
✓ Perform periodic reviews to ensure all external assets are properly managed.

Real-World Result:
Better asset visibility, enhanced security, and a more streamlined audit process.

60. No Process for Decommissioning IT Assets

📌 **Clause:** 8.2.6 – Decommissioning

What's Going Wrong:
IT assets that are no longer in use are not properly decommissioned, leading to obsolete assets being left in the system or not removed from inventory.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires proper decommissioning of IT assets to ensure they are removed from the inventory and that any sensitive data is securely erased.

How to Fix It:
✓ Implement a decommissioning process that includes data wiping, secure disposal, and asset tracking.
✓ Ensure that all assets are removed from the ITAM system upon decommissioning.
✓ Conduct periodic reviews to identify and properly retire obsolete assets.

Real-World Result:
Improved security, better data protection, and enhanced compliance with decommissioning standards.

61. Failure to Track Asset Maintenance and Upgrades

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

What's Going Wrong:
Maintenance and upgrades to IT assets are not consistently tracked, leading to gaps in asset management and potential compliance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that maintenance and upgrades be tracked as part of the asset lifecycle to ensure continued compliance and performance.

How to Fix It:
✓ Implement a system to track all maintenance activities, upgrades, and patches applied to assets.
✓ Ensure that maintenance and upgrades are recorded and linked to the

asset's history.

✓ Regularly review asset maintenance records during audits.

Real-World Result:
Improved asset performance, reduced downtime, and easier compliance verification.

62. Unclear Policies on Asset Use for Temporary Projects

📌 **Clause:** 8.2.4 – Asset Tracking and Control

What's Going Wrong:
There are no clear policies governing the use of IT assets for temporary projects, leading to misused resources or untracked assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a formal process for tracking all assets, including those used temporarily for specific projects, to ensure full accountability.

How to Fix It:
✓ Develop and implement a policy that covers the use of IT assets for temporary or short-term projects.

✓ Create a process to log and track assets assigned to temporary projects.

✓ Conduct audits to ensure assets are returned or reassigned after project completion.

Real-World Result:
Better control over temporary assets, optimized resource allocation, and improved audit accuracy.

63. Insufficient Training on ITAM Systems

📌 **Clause:** 7.3 – Awareness and Training

What's Going Wrong:
Employees are not adequately trained on IT Asset Management (ITAM) systems and processes, leading to errors in asset tracking and non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that employees be properly trained on ITAM systems and policies to ensure consistency and accuracy across asset management practices.

How to Fix It:
✓ Provide comprehensive training on ITAM systems and asset management policies for all relevant employees.
✓ Ensure ongoing training to keep employees updated on changes in ITAM tools and processes.
✓ Conduct assessments to measure employee understanding and effectiveness of training.

Real-World Result:
Improved accuracy in asset management, better audit performance, and greater employee accountability.

64. Unclear or Inconsistent Asset Tagging

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Assets are not consistently tagged with unique identifiers (e.g., barcodes, RFID tags), making it difficult to track them across their lifecycle.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires all assets to be clearly identifiable and tracked, which starts with proper tagging. Inconsistent or missing tags create compliance gaps.

How to Fix It:
✓ Ensure all physical and virtual assets are tagged with unique identifiers.
✓ Regularly audit asset tags to ensure they are intact and legible.
✓ Use automated tools to track assets based on their identifiers.

Real-World Result:
Better asset tracking, improved accountability, and a streamlined audit process.

65. No Formal Process for Software Reinstallation and Transfers

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

What's Going Wrong:
There is no formal process for reinstalling or transferring software from one device or user to another, leading to untracked software usage and potential compliance violations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that software installations be properly tracked to ensure compliance with licensing agreements.

How to Fix It:
✓ Implement a standardized process for software reinstallation and transfers.
✓ Use software tracking tools to monitor reassignments and installations.
✓ Ensure that software licenses are transferred or reassigned according to the terms of the agreement.

Real-World Result:
Improved software license management, reduced risk of non-compliance, and better audit results.

66. Failure to Identify and Manage End-of-Life (EOL) Assets

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

What's Going Wrong:
Assets approaching the end of their useful life are not identified or properly managed, leading to security risks and potential compliance issues when they are retired.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that end-of-life assets be handled according to established processes to ensure compliance with security and data protection standards.

How to Fix It:
✓ Identify assets that are nearing the end of their lifecycle and plan for their decommissioning or disposal.

✓ Implement secure data destruction processes for assets being retired.
✓ Regularly review asset lifecycle status to ensure timely retirement.

Real-World Result:
Better asset management, improved data security, and a more efficient asset retirement process.

67. No Centralized Repository for IT Asset Documentation

📌 **Clause:** 7.5 – Documented Information

What's Going Wrong:
IT asset documentation is scattered across different systems or departments, making it difficult to access and manage important information.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT asset documentation be centrally stored and easily accessible to ensure compliance and audit readiness.

How to Fix It:
✓ Create a centralized repository for all IT asset documentation.
✓ Ensure that all relevant asset information (e.g., licenses, contracts, maintenance records) is stored in this repository.
✓ Implement version control to ensure that the most up-to-date documentation is available.

Real-World Result:
Improved access to asset documentation, streamlined audits, and better compliance tracking.

68. No Defined Process for Decommissioning Cloud Resources

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

What's Going Wrong:
Cloud resources, such as virtual machines or storage, are not decommissioned according to established procedures, leading to unnecessary costs or security vulnerabilities.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT assets, including cloud resources, be decommissioned and removed from the asset register when no longer in use.

How to Fix It:
✓ Implement a formal decommissioning process for cloud resources.
✓ Ensure that cloud resources are removed from the ITAM system once they are no longer needed.
✓ Use cloud management tools to track and decommission unused resources automatically.

Real-World Result:
Reduced cloud costs, improved security, and better resource management.

69. Inconsistent Handling of Software Patches and Updates

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

What's Going Wrong:
Software patches and updates are not consistently applied, leading to security vulnerabilities and non-compliance with vendor agreements.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all software be kept up-to-date with the latest patches to ensure security and compliance.

How to Fix It:
✓ Establish a process for tracking and applying software patches and updates in a timely manner.
✓ Use automated tools to ensure that patches are applied consistently across all systems.
✓ Regularly review patch management procedures during internal audits.

Real-World Result:
Improved software security, compliance with vendor requirements, and fewer vulnerabilities.

70. Lack of Formal Process for Managing ITAM Risks

📌 **Clause:** 6.1 – Risk Management

What's Going Wrong:
Risks related to IT asset management (such as unauthorized software installations or security breaches) are not formally identified or addressed.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes risk management and requires that ITAM risks be actively identified, assessed, and mitigated.

How to Fix It:
✓ Develop a formal process for identifying, assessing, and mitigating ITAM-related risks.
✓ Integrate risk management into ITAM policies and practices.
✓ Regularly review and update risk assessments based on changing business needs and threats.

Real-World Result:
Improved risk mitigation, stronger compliance, and a more resilient ITAM system.

71. No Clear Process for Managing Software Contracts

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

What's Going Wrong:
Software contracts are not systematically managed, leading to expired agreements, missed renewals, and potential non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all software contracts be properly managed and monitored for compliance with licensing terms.

How to Fix It:
✓ Establish a process for managing all software contracts, including tracking renewal dates, terms, and conditions.
✓ Use contract management software to centralize contract information and ensure timely renewals.
✓ Ensure regular reviews of all contracts to identify compliance risks or opportunities for negotiation.

Real-World Result:
Better compliance, reduced risk of contract breaches, and optimized contract negotiations.

72. No Integration Between ITAM and Incident Management Systems

📌 **Clause:** 8.2.5 – Integration and Alignment

What's Going Wrong:
IT Asset Management (ITAM) and incident management systems are not integrated, leading to a lack of visibility and delayed responses to issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 emphasizes the integration of ITAM with other IT management processes, including incident management, to ensure assets are managed effectively.

How to Fix It:
✓ Integrate ITAM with incident management systems to track issues and their impact on assets.
✓ Ensure asset records are updated in real-time when incidents are reported.
✓ Implement a system to track the resolution of asset-related incidents.

Real-World Result:
Faster issue resolution, better asset visibility, and more efficient IT operations.

73. No Automated Alerts for Software License Violations

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

What's Going Wrong:
There is no system in place to automatically alert the team when software license violations or potential breaches occur.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires automated processes to detect and alert organizations of software license violations, ensuring timely corrective action.

How to Fix It:
✓ Implement software license management tools that include automated alerts for violations or overages.
✓ Set up automated notifications for upcoming license renewals, expirations, or overuse.
✓ Regularly monitor software deployments and usage against license terms.

Real-World Result:
Reduced risk of non-compliance and penalties, better license management, and improved audit outcomes.

74. No Continuous Monitoring of Asset Performance

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

What's Going Wrong:
There is no ongoing monitoring of IT asset performance, leading to missed opportunities for optimization and performance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires continuous monitoring and measurement of asset performance to ensure optimal utilization and compliance.

How to Fix It:
✓ Implement tools to continuously monitor asset performance, including hardware utilization, software usage, and license compliance.
✓ Use analytics to identify underused assets and reallocate them as needed.

✓ Regularly review performance metrics to ensure that assets are operating at peak efficiency.

Real-World Result:
Improved resource allocation, better asset performance, and optimized IT infrastructure.

75. No Defined Process for Managing IT Asset Data in Mergers

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

What's Going Wrong:
During mergers or acquisitions, IT asset data is not integrated or managed properly, leading to discrepancies and difficulties in tracking assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that asset data be reconciled and integrated during mergers to maintain an accurate and compliant asset management system.

How to Fix It:
✓ Implement a structured process for integrating IT asset data during mergers or acquisitions.
✓ Reconcile asset inventories from both organizations and identify duplicate or unnecessary assets.
✓ Update asset records to reflect the new structure post-merger.

Real-World Result:
A smoother merger process, better asset integration, and clearer asset records.

76. No Defined Policy for Managing Non-IT Assets

📌 **Clause:** 8.1 – Asset Identification

What's Going Wrong:
Non-IT assets such as office furniture, physical equipment, or other business assets are not properly managed or tracked.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all business assets, not just IT-related ones, be tracked and managed effectively to ensure compliance.

How to Fix It:
✓ Develop a policy for managing all non-IT assets, including inventory and lifecycle management.
✓ Include non-IT assets in the asset management system for visibility and control.
✓ Regularly update records for all assets, including physical items like equipment or office furniture.

Real-World Result:
Better visibility and management of all assets, improved asset lifecycle tracking, and enhanced overall asset control.

77. Insufficient Backup and Recovery of IT Asset Data

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

What's Going Wrong:
IT asset data, including software and hardware records, is not backed up or properly protected, leading to potential data loss.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all critical asset data be properly backed up and accessible in case of a disaster or audit review.

How to Fix It:
✓ Implement a robust backup system for IT asset data, ensuring that all records are regularly backed up.
✓ Store backups in secure, off-site locations or cloud-based storage.
✓ Regularly test backup and recovery processes to ensure data integrity and availability.

Real-World Result:
Better data security, reduced risk of data loss, and ensured access to asset records during audits.

78. No Lifecycle Management for Digital Assets

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

What's Going Wrong:
Digital assets such as virtual machines, cloud services, and digital licenses are not managed through their full lifecycle, leading to inefficiencies and increased risk.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates that all assets, including digital ones, be tracked and managed from procurement to decommissioning.

How to Fix It:
✓ Implement lifecycle management for all digital assets, including cloud resources and virtual environments.
✓ Track each asset through its full lifecycle, from provisioning to retirement.

✓ Regularly review digital assets to ensure they are compliant and properly retired when no longer needed.

Real-World Result:
Better control of digital assets, improved efficiency, and enhanced security.

79. Failure to Monitor IT Asset Depreciation

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

What's Going Wrong:
The depreciation of IT assets is not monitored or updated regularly, leading to inaccurate financial reporting and compliance gaps.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that IT assets be accurately depreciated over their lifecycle to ensure that financial records reflect true asset values.

How to Fix It:
✓ Set up a system to track and update the depreciation of assets based on their lifecycle and usage.
✓ Ensure that depreciation schedules are integrated with the financial system for accurate reporting.
✓ Regularly review depreciation practices and adjust them as needed.

Real-World Result:
More accurate financial records, improved asset management, and better audit outcomes.

80. No Clear Process for Managing Software in Virtualized Environments

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

What's Going Wrong:
Software used in virtualized environments (e.g., virtual machines, containers) is not tracked or managed separately from physical assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires all software, including those running in virtualized environments, to be properly tracked and managed to ensure compliance with licensing agreements.

How to Fix It:
✓ Implement tracking tools for software used in virtualized environments.
✓ Separate virtualized and physical software in the asset management system to ensure clarity.
✓ Regularly audit virtualized environments to ensure license compliance.

Real-World Result:
Improved license compliance, better control over virtualized assets, and fewer audit issues.

81. No Process for Managing IT Asset Borrowing Across Teams

📌 **Clause:** 8.2.2 – Asset Control

What's Going Wrong:
Assets borrowed by different teams or departments are not tracked, leading to unaccounted-for assets or potential misuse.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, including those temporarily borrowed across departments, be tracked to ensure full accountability.

How to Fix It:

✓ Implement a formal asset borrowing and tracking policy for all departments.

✓ Use asset management software to record borrowing transactions and return dates.

✓ Periodically review asset borrowing logs to ensure proper returns.

Real-World Result:

Improved asset visibility, better tracking, and fewer missing or misused assets.

82. Inadequate Tracking of Software Updates and Patches

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

What's Going Wrong:

Software updates and patches are not consistently tracked or managed, leading to security vulnerabilities and non-compliance with vendor requirements.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires that software patches and updates be applied and tracked to ensure software integrity and compliance.

How to Fix It:

✓ Implement an automated system for tracking software updates and patches.

✓ Establish a policy to apply updates regularly and document them in the ITAM system.

✓ Regularly review patch management procedures and update them as needed.

Real-World Result:
Improved software security, better license compliance, and reduced vulnerabilities.

83. Failure to Include Mobile and IoT Devices in IT Asset Management

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

What's Going Wrong:
Mobile devices (e.g., smartphones, tablets) and Internet of Things (IoT) devices are not tracked within the ITAM system, leading to a lack of visibility and potential security risks.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires all IT assets, including mobile and IoT devices, to be tracked for security and compliance purposes.

How to Fix It:
✓ Ensure that all mobile and IoT devices are included in the asset inventory.
✓ Use device management tools to track mobile and IoT devices throughout their lifecycle.
✓ Regularly audit mobile and IoT devices to ensure compliance with security policies.

Real-World Result:
Better control over mobile and IoT devices, improved security, and reduced compliance risks.

84. No Clear Asset Classification System for High-Risk Assets

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

What's Going Wrong:
High-risk assets, such as sensitive data storage devices, are not properly classified or assigned additional controls.

Why It Matters During an Audit:
ISO/IEC 19770-1 mandates that all assets, particularly high-risk ones, be classified and tracked to ensure appropriate security measures are in place.

How to Fix It:
✓ Develop and implement an asset classification system based on risk levels and criticality.
✓ Assign additional controls (e.g., stricter access, enhanced security) for high-risk assets.
✓ Review and update asset classifications regularly.

Real-World Result:
Stronger protection of critical assets, improved compliance, and reduced audit findings.

85. No Process for Managing Third-Party Software

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

What's Going Wrong:
Third-party software is not adequately tracked or managed, leading to potential licensing issues, compliance violations, or security vulnerabilities.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that third-party software be tracked and

managed just like any other software asset to ensure compliance and avoid risks.

How to Fix It:

✓ Implement a process to track and manage all third-party software.

✓ Regularly audit third-party software to ensure compliance with licensing terms.

✓ Ensure that third-party software is included in the ITAM system for visibility and control.

Real-World Result:

Improved software compliance, reduced risk of vendor disputes, and better control over third-party assets.

86. Failure to Track Software Usage in Virtualized Environments

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

What's Going Wrong:

Software usage in virtualized environments is not monitored, leading to overuse or non-compliance with license agreements.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires all software, including that running in virtual environments, to be tracked and managed to ensure license compliance.

How to Fix It:

✓ Implement software usage tracking tools for virtualized environments.

✓ Ensure that all virtual machines and containers are included in the asset management system.

✓ Regularly audit virtualized environments for software compliance.

Real-World Result:
Better compliance and license optimization in virtualized environments, reducing audit risks.

87. No Integration Between ITAM and Financial Systems for Depreciation

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

What's Going Wrong:
There is no integration between ITAM and financial systems, resulting in discrepancies between asset value depreciation and financial records.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that asset depreciation be properly tracked and aligned with financial systems to ensure accurate reporting.

How to Fix It:
✓ Integrate ITAM and financial systems to automatically track depreciation.
✓ Ensure asset values are updated in both systems regularly.
✓ Reconcile depreciation schedules and asset values during internal audits.

Real-World Result:
More accurate financial reporting, improved asset management, and smoother audits.

88. Inadequate Tracking of Software Usage in Multi-Location Environments

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

What's Going Wrong:
Software usage across multiple locations is not tracked consistently, leading to potential compliance violations and unoptimized software use.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires consistent tracking of software across all locations to ensure accurate compliance with licensing agreements.

How to Fix It:
✓ Implement software tracking systems that can monitor usage across multiple locations.
✓ Ensure that software deployment and usage data is centralized for visibility.
✓ Regularly audit software usage across all business locations.

Real-World Result:
Better software utilization, reduced compliance risks, and more efficient use of resources.

89. No Clear Policy for IT Asset Disposals and Recycling

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

What's Going Wrong:
There is no clear policy for disposing of or recycling old IT assets, leading to potential data breaches or environmental violations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires a documented and secure disposal process for IT assets to ensure data protection and environmental compliance.

How to Fix It:
✓ Develop a formal asset disposal and recycling policy that includes secure data wiping and environmental compliance.
✓ Use certified e-waste disposal vendors for asset destruction.
✓ Maintain records of all disposals and recycling activities.

Real-World Result:
Improved data security, better environmental compliance, and reduced risk during audits.

90. No Automated Software License Compliance Tracking

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

What's Going Wrong:
Software license compliance is tracked manually, which increases the risk of errors and missed violations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires automated systems to track and ensure software license compliance. Manual processes can lead to inaccuracies and potential non-compliance.

How to Fix It:
✓ Implement automated software license tracking tools that monitor usage in real-time.
✓ Integrate license tracking tools with other asset management systems.
✓ Use automated reporting to generate compliance reports for internal or external audits.

Real-World Result:
Streamlined software license compliance, fewer errors, and faster audits.

91. Lack of Asset Management Training for New Employees

📌 **Clause:** 7.3 – Awareness and Training

What's Going Wrong:
New employees are not adequately trained on IT asset management processes, leading to inconsistent practices and potential non-compliance.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all relevant employees be trained on asset management policies to ensure consistent practices and compliance.

How to Fix It:
✓ Develop a training program for new employees focused on ITAM processes.
✓ Include ITAM training in the onboarding process for all employees handling assets.
✓ Conduct periodic refresher courses to ensure ongoing awareness and compliance.

Real-World Result:
Improved consistency in asset management, better compliance, and reduced audit issues.

92. No Formal Process for Managing Software Patching in Virtual Environments

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

What's Going Wrong:
Software patches are not consistently applied in virtualized environments, leading to vulnerabilities and compliance issues.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all software, including those in virtualized environments, be maintained with the latest security patches and updates.

How to Fix It:
✓ Implement a patch management system that tracks software patches for virtualized environments.
✓ Ensure that all virtual machines and containers receive timely updates.
✓ Regularly audit virtualized environments to ensure compliance with patching policies.

Real-World Result:
Improved security, reduced compliance risks, and better virtualized asset management.

93. No System for Tracking Software License Allocations and Reassignments

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

What's Going Wrong:
Software licenses are allocated to employees without proper tracking,

leading to issues when reassigning licenses or ensuring compliance with license terms.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that software license allocations and reassignments be clearly documented to ensure accurate tracking and compliance.

How to Fix It:
✓ Implement a system that tracks software license assignments and reassignments in real-time.
✓ Use automated tools to ensure that licenses are properly reallocated when employees change roles or leave.
✓ Regularly reconcile software usage to ensure compliance with license terms.

Real-World Result:
Optimized software license allocation, improved license compliance, and streamlined audits.

94. No Defined Criteria for Asset Classification and Prioritization

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

What's Going Wrong:
Assets are not classified or prioritized based on value or criticality, making it difficult to allocate appropriate resources or implement necessary controls.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that assets be classified based on their importance, with higher-value or critical assets receiving enhanced controls and oversight.

How to Fix It:

✓ Develop a classification system that categorizes assets based on criticality, value, and usage.

✓ Prioritize high-value or sensitive assets for more frequent monitoring and enhanced security measures.

✓ Regularly review asset classification to ensure it reflects current business needs.

Real-World Result:

Improved asset security, more efficient resource allocation, and better audit outcomes.

95. Incomplete Asset Recovery Process After System Upgrades

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

What's Going Wrong:

Assets are not properly recovered or reassigned after system upgrades or hardware replacements, leading to missing or untracked equipment.

Why It Matters During an Audit:

ISO/IEC 19770-1 requires that all assets be recovered, reassigned, or retired properly to ensure proper asset control and accountability.

How to Fix It:

✓ Implement a formal process for asset recovery after system upgrades or hardware replacements.

✓ Track all assets that are replaced, reassigned, or decommissioned.

✓ Ensure all recovered assets are properly inventoried and reassigned or retired.

Real-World Result:
Reduced asset loss, better resource management, and more accurate asset records.

96. Lack of Regular Internal Audits of ITAM Processes

📌 **Clause:** 9.2 – Internal Audit

What's Going Wrong:
Internal audits of IT asset management processes are not conducted regularly, making it difficult to identify gaps or inefficiencies in asset management practices.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that internal audits be performed regularly to ensure the effectiveness and compliance of ITAM processes.

How to Fix It:
✓ Schedule regular internal audits of ITAM processes to identify and resolve non-conformities.
✓ Use audit results to continuously improve asset management practices.
✓ Ensure audits are comprehensive and include all relevant assets and processes.

Real-World Result:
Proactive identification and resolution of issues, leading to improved compliance and smoother audits.

97. No Process for Tracking and Managing Asset Warranties

📌 **Clause:** 8.2 – Asset Management Lifecycle

What's Going Wrong:
Asset warranties, such as those for hardware, are not tracked, leading to missed opportunities for repairs, replacements, or service claims.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that warranties be tracked as part of the asset management lifecycle to ensure assets are maintained properly and any claims can be made.

How to Fix It:
✓ Implement a process for tracking asset warranties, including expiration dates and service terms.
✓ Ensure warranties are linked to asset records in the ITAM system.
✓ Regularly review warranty statuses and claim opportunities for assets nearing the end of their warranty period.

Real-World Result:
Better management of warranties, reduced repair costs, and improved asset lifecycle management.

98. No Process for Managing Vendor-Provided IT Assets

📌 **Clause:** 8.2.6 – Procurement and Vendor Management

What's Going Wrong:
IT assets provided by vendors (e.g., leased equipment, third-party software) are not properly tracked, leading to mismanagement and potential compliance violations.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all assets, including those provided by vendors, be properly tracked and managed to ensure accountability and compliance.

How to Fix It:
✓ Develop a process for tracking and managing vendor-provided IT assets.
✓ Ensure that all vendor assets are included in the ITAM system and treated with the same level of control as owned assets.
✓ Regularly audit vendor-provided assets for compliance and proper usage.

Real-World Result:
Improved control over vendor assets, better compliance, and reduced vendor disputes.

99. No Integration Between ITAM and Procurement Systems

📌 **Clause:** 8.2.5 – Integration and Alignment

What's Going Wrong:
IT asset management and procurement systems are not integrated, leading to inconsistent tracking and inefficiencies in asset management.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that procurement and ITAM systems be aligned to ensure assets are properly tracked from the point of purchase through their lifecycle.

How to Fix It:
✓ Integrate ITAM systems with procurement software for real-time asset tracking.
✓ Ensure all assets procured through external vendors are automatically recorded in the ITAM system.

✓ Periodically review procurement and ITAM integration to ensure smooth data flow.

Real-World Result:
Streamlined asset management processes, better compliance, and more efficient use of resources.

100. No Asset Management Strategy for Emerging Technologies

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

What's Going Wrong:
Emerging technologies, such as AI, blockchain, and IoT, are not incorporated into the asset management strategy, leading to untracked or poorly managed assets.

Why It Matters During an Audit:
ISO/IEC 19770-1 requires that all IT assets, including those related to emerging technologies, be managed and tracked to ensure compliance and security.

How to Fix It:
✓ Develop an asset management strategy that includes emerging technologies.
✓ Identify all assets related to new technologies and track them through their lifecycle.
✓ Implement tools and processes that integrate these emerging technologies into the broader ITAM framework.

Real-World Result:
Improved control over emerging technology assets, better risk management, and more agile asset management strategies.

Achieving ISO/IEC 19770-1 Compliance

Achieving and maintaining ISO/IEC 19770-1 compliance is an ongoing journey.

By addressing these 100 common non-conformities, your organization can build a stronger, more resilient IT Asset Management (ITAM) system, reduce audit risks, and ensure that all assets are effectively tracked and optimized.

This guide has provided a comprehensive roadmap for addressing the most common failures and offering practical solutions. Start implementing these fixes today to achieve better software license compliance, cloud resource management, and asset security.

Stay proactive, stay compliant, and let your ITAM practices drive organizational success.

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