100 Common Non-Conformities in ISO 27001 Audits

A Practical Guide to Identifying, Understanding, and Fixing the Most Common ISO 27001 Audit Issues

Objectives of this guide:

Achieving ISO 27001 compliance strengthens an organization's information security management system (ISMS) and builds trust with stakeholders.

However, many businesses struggle with common audit non-conformities that can delay certification.

This guide highlights 100 frequent non-conformities with practical insights on how to fix them.

✓ Identify and address common ISO 27001 non-conformities before audits.
✓ Provide real-world scenarios to illustrate security gaps.
✓ Deliver actionable solutions for effective compliance.
✓ Promote cybersecurity best practices in risk management, access control, and incident response.
✓ Support continuous improvement for ISMS teams, IT professionals, and auditors.

This guide is ideal for:

- CISOs, security managers, and IT professionals preparing for an audit.
- Compliance teams working to close security gaps.
- Consultants and auditors assisting in ISO 27001 certification.
- Business leaders aiming to align security with industry standards.

Use this resource to take a proactive approach to compliance, streamline audits, and build a resilient security framework.

1. No defined risk management procedure

📌 **ISO 27001 Section: 6.1.2 – Information security risk assessment**
🔍 **Scenario:** A company handling sensitive customer data does not have a formal process to identify and manage information security risks. When asked, employees rely on ad-hoc decisions rather than a structured risk assessment framework.
❓ **What is missing?** A structured, well-documented risk management process outlining risk identification, evaluation, and treatment strategies is absent.
💡 **How to fix?** Develop a formalized risk management framework, including documented risk assessment methodologies, evaluation criteria, and periodic risk reviews. Ensure risk registers are updated regularly and linked to mitigation actions.

2. Weak risk treatment evidence

📌 **ISO 27001 Section: 6.1.3 – Information security risk treatment**
🔍 **Scenario:** During an ISO 27001 audit, the auditor requests proof of implemented risk treatments. However, the organization fails to provide concrete records, relying on informal discussions.
❓ **What is missing?** There is no clear documentation of risk treatment plans, actions taken, or assigned responsibilities.
💡 **How to fix?** Maintain a risk treatment plan that details mitigation measures, assigned owners, and timelines. Implement a structured system to track and validate risk treatment actions.

3. No scheduled internal audits or management reviews

📌 **ISO 27001 Section: 9.2 & 9.3 – Internal audit & Management review**

🔍 **Scenario:** An organization has not conducted an internal audit or a management review in the past year, making it difficult to evaluate ISMS effectiveness.

❓ **What is missing?** A documented schedule and execution of internal audits and management reviews are absent.

💡 **How to fix?** Establish a structured schedule for conducting internal audits at least annually. Document audit findings, corrective actions, and involve top management in periodic ISMS reviews.

4. Weak Statement of Applicability (SoA)

📌 **ISO 27001 Section: 6.1.3 (d) – Statement of Applicability**

🔍 **Scenario:** An organization presents an SoA that is outdated, lacks justifications for excluded Annex A controls, and does not align with its risk assessment.

❓ **What is missing?** A clear, up-to-date SoA that reflects applicable controls and provides valid justifications for exclusions.

💡 **How to fix?** Regularly update the SoA to align with risk assessments, justify excluded controls, and maintain consistency with the organization's security measures.

5. No performance metrics for ISMS

📌 **ISO 27001 Section: 9.1 – Monitoring, measurement, analysis, and evaluation**

🔍 **Scenario:** The organization cannot demonstrate measurable improvements in its ISMS because it lacks defined performance indicators.

❓ **What is missing?** There are no key performance indicators (KPIs) to evaluate ISMS effectiveness.

💡 **How to fix?** Define measurable security objectives, such as incident reduction rates, compliance scores, and employee training completion, and review them regularly.

6. Poor incident management process

📌 **ISO 27001 Section: A.5.24 – Information security incident management**

🔍 **Scenario:** Employees report security incidents verbally, but there is no structured system for tracking, resolving, and learning from them.

❓ **What is missing?** A formal incident management process, including defined reporting channels, response teams, and post-incident analysis.

💡 **How to fix?** Implement a documented incident response process with clear reporting mechanisms, response team roles, and structured post-incident reviews.

7. Weak access control measures

📌 **ISO 27001 Section: A.8.2 & A.8.3 – Identity and access management**

🔍 **Scenario:** Former employees and third-party contractors still have

access to company systems, increasing the risk of unauthorized access.
❓ **What is missing?** Periodic access reviews and enforcement of least privilege access.
💡 **How to fix?** Implement a strict access control policy, conduct quarterly access reviews, and enforce multi-factor authentication (MFA) for sensitive systems.

8. Lack of supplier security management

📌 **ISO 27001 Section: A.5.19 – Supplier relationship management**
🔍 **Scenario:** A company relies on third-party vendors for data processing but has no security agreements or assessments in place.
❓ **What is missing?** A structured supplier security assessment and contractual obligations ensuring compliance.
💡 **How to fix?** Establish supplier security assessment procedures, enforce security clauses in contracts, and conduct periodic vendor audits.

9. Insufficient personnel awareness and training

📌 **ISO 27001 Section: A.6.3 – Awareness, education, and training**
🔍 **Scenario:** Employees regularly fall for phishing scams, indicating a lack of security awareness training.
❓ **What is missing?** Structured security awareness programs and employee training tracking.
💡 **How to fix?** Conduct regular security training sessions, phishing simulations, and track participation to ensure continuous learning.

10. No up-to-date inventory of information assets

📌 **ISO 27001 Section: A.5.9 & A.8.1.1 – Inventory of assets**
🔍 **Scenario:** An organization struggles to identify critical information assets during an audit because no centralized inventory exists.
❓ **What is missing?** A well-documented and updated inventory of information assets.
💡 **How to fix?** Maintain an up-to-date asset register, assign ownership, classify assets based on risk, and regularly review the inventory.

11. No business continuity testing

📌 **ISO 27001 Section: A.5.29 – Business Continuity Planning**
🔍 **Scenario:** An organization has a business continuity plan (BCP) in place but has never tested it, resulting in uncertainty about its effectiveness.
❓ **What is missing?** Regular testing of the BCP to ensure its effectiveness during a real crisis.
💡 **How to fix?** Conduct periodic BCP drills, simulate real-world scenarios, and document test results for continuous improvements.

12. Lack of encryption for sensitive data

📌 **ISO 27001 Section: A.5.13 – Encryption**
🔍 **Scenario:** Sensitive customer data is stored in plaintext on internal databases, making it vulnerable to unauthorized access.
❓ **What is missing?** Implementation of encryption mechanisms for data at rest and in transit.

💡 **How to fix?** Enforce encryption policies, utilize strong encryption standards, and ensure key management procedures are in place.

13. No formal change management process

📌 **ISO 27001 Section: A.5.32 – Change Management**
🔍 **Scenario:** IT infrastructure changes are made without prior approval, leading to security vulnerabilities.
❓ **What is missing?** A structured change management process with approvals and risk assessments.
💡 **How to fix?** Implement a documented change management policy, including impact assessments and approval workflows.

14. Weak backup management

📌 **ISO 27001 Section: A.5.30 – Backup and Recovery**
🔍 **Scenario:** Backups exist but have never been tested, causing uncertainty about data recovery capabilities.
❓ **What is missing?** Regular backup testing and verification procedures.
💡 **How to fix?** Schedule automated backups, test recovery processes periodically, and document test results.

15. Failure to document information security policies

📌 **ISO 27001 Section: 5.2 – Information Security Policies**
🔍 **Scenario:** Employees are unaware of security policies due to a lack of formal documentation.

❓ **What is missing?** A structured, documented information security policy.
💡 **How to fix?** Develop and distribute security policies, conduct training sessions, and enforce compliance through regular reviews.

16. No data retention and disposal policy

📌 **ISO 27001 Section: A.5.12 – Data Retention & Disposal**
🔍 **Scenario:** An organization stores customer data indefinitely without a clear policy on retention or disposal. During an audit, they are unable to demonstrate compliance with regulatory requirements such as GDPR, which mandates that data should not be stored longer than necessary.
❓ **What is missing?** A well-defined data retention and disposal policy specifying how long different types of data should be kept and when and how they should be securely deleted.
💡 **How to fix?** Develop a documented data retention policy that defines retention periods for various data categories, including business, legal, and regulatory requirements. Implement secure deletion methods such as data wiping or physical destruction and ensure employees follow the disposal process through regular training.

17. Inadequate control over removable media

📌 **ISO 27001 Section: A.5.14 – Control of Removable Media**
🔍 **Scenario:** Employees frequently use USB drives and external hard drives to transfer sensitive company data. There is no tracking mechanism, and lost or stolen drives have led to data breaches in the past. The organization does not have a formal policy on removable media usage.
❓ **What is missing?** A strict policy governing the use of removable media, including encryption requirements and access controls.

💡 **How to fix?** Implement a removable media control policy that limits the use of USB drives and mandates encryption for all data transferred via removable media. Introduce logging mechanisms to track removable media usage and deploy endpoint security solutions that restrict unauthorized devices from connecting to corporate systems.

18. No third-party audit agreements

📌 **ISO 27001 Section: A.5.20 – Managing Security of Supplier Services**
🔍 **Scenario:** The organization relies on third-party vendors to process sensitive customer data but has no agreement requiring them to undergo regular security audits. An external security breach linked to one of their suppliers puts customer information at risk.
❓ **What is missing?** A formal supplier security assessment and contractual obligations ensuring compliance with security best practices.
💡 **How to fix?** Establish security clauses in vendor agreements that require third-party audits, compliance with ISO 27001 standards, and adherence to security policies. Conduct periodic risk assessments for high-risk suppliers and enforce penalties for non-compliance. Require vendors to provide security reports and certifications as proof of their compliance efforts.

19. Uncontrolled use of personal devices

📌 **ISO 27001 Section: A.5.15 – Bring Your Own Device (BYOD) Security**
🔍 **Scenario:** Employees use personal smartphones and laptops to access corporate networks without security controls. One employee loses a personal laptop containing confidential company data, leading to a

potential security breach.

❓ **What is missing?** A Bring Your Own Device (BYOD) policy that defines security requirements for personal devices accessing corporate resources.
💡 **How to fix?** Implement a BYOD policy requiring personal devices to comply with security standards such as password protection, encryption, and remote wiping capabilities. Enforce Mobile Device Management (MDM) solutions to monitor and control device access. Restrict access to sensitive data based on device compliance and ensure employees acknowledge security responsibilities before using personal devices for work.

20. Poor patch management process

📌 **ISO 27001 Section: A.5.23 – Patch Management & Vulnerability Management**
🔍 **Scenario:** The IT department frequently delays installing security patches for critical systems due to a lack of proper scheduling. A recent cyberattack exploited a known vulnerability that had a patch available months ago.
❓ **What is missing?** A structured patch management process to ensure timely application of security updates.
💡 **How to fix?** Implement an automated patch management system that monitors and deploys security updates as soon as they are released. Establish a patching schedule for routine updates and emergency patches for critical vulnerabilities. Maintain a vulnerability tracking system to assess patch compliance across all systems. Conduct regular vulnerability scans to identify unpatched systems and enforce accountability for timely updates.

20. Poor patch management process

📌 **ISO 27001 Section: A.5.23 – Patch Management & Vulnerability Management**

🔍 **Scenario:** The IT department frequently delays installing security patches for critical systems due to a lack of proper scheduling. A recent cyberattack exploited a known vulnerability that had a patch available months ago.

❓ **What is missing?** A structured patch management process to ensure timely application of security updates.

💡 **How to fix?** Implement an automated patch management system that monitors and deploys security updates as soon as they are released. Establish a patching schedule for routine updates and emergency patches for critical vulnerabilities. Maintain a vulnerability tracking system to assess patch compliance across all systems. Conduct regular vulnerability scans to identify unpatched systems and enforce accountability for timely updates.

21. No disaster recovery plan (DRP)

📌 **ISO 27001 Section: A.5.28 – Disaster Recovery Planning**

🔍 **Scenario:** A major server crash leads to extended downtime, and the IT team has no structured process to restore services efficiently. Critical business functions are impacted, causing financial losses and customer dissatisfaction.

❓ **What is missing?** A documented disaster recovery plan that outlines steps for restoring IT operations after a major disruption.

💡 **How to fix?** Develop a detailed DRP that includes roles and responsibilities, recovery time objectives (RTOs), recovery point objectives (RPOs), backup procedures, and testing schedules. Conduct regular DRP

drills to validate the effectiveness of recovery strategies and ensure all stakeholders are prepared for emergency situations.

22. No role-based access control (RBAC)

📌 **ISO 27001 Section: A.8.2 – Identity & Access Management**
🔍 **Scenario:** Employees in different departments have access to unnecessary systems and data beyond their job roles. A junior employee accidentally deletes a critical database due to unrestricted admin privileges.
❓ **What is missing?** A role-based access control (RBAC) mechanism to limit user permissions based on job roles.
💡 **How to fix?** Implement an RBAC model where employees are assigned specific access levels according to their job functions. Review access privileges regularly and remove unnecessary permissions. Use an identity and access management (IAM) system to automate access provisioning and revocation based on employment status and role changes.

23. Weak authentication mechanisms

📌 **ISO 27001 Section: A.8.3 – Authentication Security**
🔍 **Scenario:** Employees log in using weak passwords such as "123456" or "password," making the system vulnerable to brute-force attacks. Some systems do not require multi-factor authentication (MFA) for remote access.
❓ **What is missing?** Strong authentication mechanisms to prevent unauthorized access.
💡 **How to fix?** Implement strict password policies that require complexity, length, and periodic changes. Enforce multi-factor authentication (MFA) for all critical systems and remote access points. Introduce password managers

to help employees manage and generate secure passwords. Conduct periodic audits to identify weak passwords and enforce compliance with authentication best practices.

24. Failure to review firewall rules periodically

📌 **ISO 27001 Section: A.5.17 – Network Security Management**
🔍 **Scenario:** The organization has had the same firewall rules in place for years without review. Unused and overly permissive rules create potential security loopholes, allowing unauthorized access to internal systems.
❓ **What is missing?** A structured review process for firewall rules to ensure they are up to date and aligned with current security policies.
💡 **How to fix?** Establish a periodic firewall rule review process, ensuring that outdated, unnecessary, or overly permissive rules are removed or adjusted. Implement firewall monitoring tools to log and analyze traffic patterns. Require security teams to assess firewall configurations regularly and align them with evolving business and security requirements.

25. No security review of new IT projects

📌 **ISO 27001 Section: A.5.33 – Secure Development & Change Management**
🔍 **Scenario:** The IT team launches new applications and cloud-based solutions without conducting security assessments. A newly deployed web application is later found to be vulnerable to SQL injection attacks.
❓ **What is missing?** A mandatory security review process for new IT projects before deployment.
💡 **How to fix?** Integrate security assessments into the project lifecycle. Conduct threat modeling, vulnerability assessments, and penetration

testing before launching new IT systems. Establish a secure software development lifecycle (SDLC) that includes security checkpoints and approval requirements. Ensure that security teams are involved in IT project planning from the beginning to address potential risks early.

25. No security review of new IT projects

📌 **ISO 27001 Section: A.5.33 – Secure Development & Change Management**

🔍 **Scenario:** The IT team launches new applications and cloud-based solutions without conducting security assessments. A newly deployed web application is later found to be vulnerable to SQL injection attacks.

❓ **What is missing?** A mandatory security review process for new IT projects before deployment.

💡 **How to fix?** Integrate security assessments into the project lifecycle. Conduct threat modeling, vulnerability assessments, and penetration testing before launching new IT systems. Establish a secure software development lifecycle (SDLC) that includes security checkpoints and approval requirements. Ensure that security teams are involved in IT project planning from the beginning to address potential risks early.

26. Insufficient logging and monitoring

📌 **ISO 27001 Section: A.5.27 – Security Monitoring**

🔍 **Scenario:** A security breach goes undetected for weeks because logs are not collected, analyzed, or reviewed regularly.

❓ **What is missing?** A robust logging and monitoring system to detect and respond to security incidents in real time.

💡 **How to fix?** Implement centralized logging with a Security Information

and Event Management (SIEM) solution to collect, analyze, and alert security teams on suspicious activities. Define log retention policies and ensure critical logs are regularly reviewed. Conduct periodic log audits to detect potential threats.

27. Lack of accountability for information security

📌 **ISO 27001 Section: 5.1 – Leadership & Commitment**
🔍 **Scenario:** The organization lacks clearly defined roles and responsibilities for information security, leading to delays in incident response and risk management.
❓ **What is missing?** Clear ownership and accountability for ISMS implementation and security-related activities.
💡 **How to fix?** Assign roles and responsibilities for security management, ensuring leadership commitment to information security. Establish a governance framework where top management actively participates in ISMS oversight. Conduct regular meetings to review security performance and drive improvements.

28. No classification of information

📌 **ISO 27001 Section: A.5.10 – Information Classification**
🔍 **Scenario:** Employees store confidential customer data in shared folders without proper access controls, increasing the risk of data leaks.
❓ **What is missing?** A formal information classification policy to define and enforce handling rules for different data types.
💡 **How to fix?** Develop a data classification framework that categorizes data based on sensitivity (e.g., public, internal, confidential, restricted).

Implement labeling mechanisms and access controls to ensure proper data protection. Train employees on handling classified information securely.

29. Weak password policies

📌 **ISO 27001 Section: A.8.2.3 – Password Management**
🔍 **Scenario:** Employees use weak and easily guessable passwords, leading to frequent unauthorized access attempts. Some systems still allow default passwords.
❓ **What is missing?** Strong password policies and enforcement mechanisms to enhance authentication security.
💡 **How to fix?** Implement a password policy that requires complexity, minimum length, expiration, and multi-factor authentication (MFA). Use password managers to help employees manage and generate strong passwords. Regularly audit password strength and enforce compliance through technical controls.

30. Lack of physical security controls

📌 **ISO 27001 Section: A.7.4 – Physical Security**
🔍 **Scenario:** Unauthorized individuals gain access to server rooms due to weak physical security controls, increasing the risk of data theft.
❓ **What is missing?** Strong physical security measures to protect critical infrastructure.
💡 **How to fix?** Implement access control mechanisms such as biometric authentication, keycards, and surveillance cameras for sensitive areas. Conduct regular security audits to assess physical security gaps and take corrective measures.

31. No employee exit process for access revocation

📌 **ISO 27001 Section: A.8.2.4 – Access Revocation**
🔍 **Scenario:** A former employee still has access to corporate email and internal systems, posing a security risk.
❓ **What is missing?** A structured process to revoke access when employees leave the organization.
💡 **How to fix?** Establish an offboarding procedure to immediately revoke system access, retrieve company assets, and disable accounts upon termination. Automate the process through an identity and access management (IAM) system.

32. Failure to conduct penetration testing

📌 **ISO 27001 Section: A.5.25 – Vulnerability Assessment & Testing**
🔍 **Scenario:** The organization has never tested its systems for vulnerabilities, leading to undetected security flaws that could be exploited.
❓ **What is missing?** Regular penetration testing and vulnerability assessments to identify weaknesses.
💡 **How to fix?** Conduct periodic penetration tests on critical systems, web applications, and networks. Hire external security experts for unbiased assessments and remediate identified vulnerabilities promptly.

33. Unsecured wireless networks

📌 **ISO 27001 Section: A.5.17 – Network Security**
🔍 **Scenario:** Employees connect to an open Wi-Fi network in the office,

making internal communications susceptible to eavesdropping.
❓ **What is missing?** Proper security controls to secure wireless networks and prevent unauthorized access.
💡 **How to fix?** Enforce WPA3 encryption, implement network segmentation, and require authentication for corporate Wi-Fi access. Disable guest networks or provide separate, restricted access for visitors.

34. No documentation of security incidents

📌 **ISO 27001 Section: A.5.24 – Incident Documentation**
🔍 **Scenario:** After a data breach, there is no record of what happened, how it was handled, or what lessons were learned.
❓ **What is missing?** A structured process to document and analyze security incidents for future improvements.
💡 **How to fix?** Develop an incident documentation procedure that records incident details, root causes, actions taken, and resolution steps. Use a centralized incident management system for tracking and reporting.

35. Outdated software versions in production

📌 **ISO 27001 Section: A.5.23 – Patch Management & Secure Configuration**
🔍 **Scenario:** The organization continues using outdated software with known vulnerabilities, increasing the risk of cyberattacks.
❓ **What is missing?** A proactive approach to software updates and security patching.
💡 **How to fix?** Establish a software update policy that mandates regular patching and upgrading of outdated applications. Implement automated tools to monitor and apply security updates across all systems.

35. Outdated software versions in production

📌 ISO 27001 Section: A.5.23 – Patch Management & Secure Configuration

🔍 **Scenario:** The organization continues using outdated software with known vulnerabilities, increasing the risk of cyberattacks. The IT team delays upgrades due to concerns about compatibility with legacy systems. As a result, hackers exploit a well-known vulnerability that had a patch released months ago, leading to data theft.

❓ **What is missing?** A proactive approach to software updates, vulnerability management, and security patching.

💡 **How to fix?** Establish a software update policy that mandates regular patching and upgrading of outdated applications. Implement automated tools to monitor, identify, and apply security updates across all systems. Schedule routine maintenance to test software updates in a controlled environment before full deployment, ensuring that upgrades do not disrupt business operations.

36. No strategy for social engineering attacks

📌 ISO 27001 Section: A.6.3 – Awareness, Education, and Training

🔍 **Scenario:** Employees frequently receive phishing emails but are unaware of how to recognize and report them. One employee clicks on a malicious link, leading to ransomware infection. The organization has no formal security awareness training or phishing simulations in place.

❓ **What is missing?** A structured program to educate employees about social engineering tactics and how to respond to suspicious activity.

💡 **How to fix?** Develop a security awareness training program focused on

social engineering threats such as phishing, vishing, and baiting. Conduct periodic simulated phishing exercises to test employee awareness. Implement clear reporting mechanisms and encourage a culture of vigilance, ensuring that employees know whom to contact when they suspect a social engineering attempt.

37. Weak email security controls

📌 **ISO 27001 Section: A.5.17 – Network Security**

🔍 **Scenario:** The organization does not enforce email security measures, allowing employees to send and receive unencrypted sensitive information. A fraudulent email impersonating a senior executive successfully tricks an employee into transferring funds to an attacker-controlled account.

❓ **What is missing?** Robust email security controls to prevent phishing, spoofing, and data leaks.

💡 **How to fix?** Enforce security policies such as email encryption, domain-based message authentication (DMARC, DKIM, SPF), and advanced spam filtering. Implement Data Loss Prevention (DLP) policies to monitor and prevent unauthorized sharing of sensitive data. Provide regular security awareness training on how to identify and report phishing attempts.

38. No mobile device management policy

📌 **ISO 27001 Section: A.5.15 – Mobile Device Security**

🔍 **Scenario:** Employees use personal and company-issued mobile devices to access corporate data, but there are no security controls in place. A lost device containing sensitive client data is not remotely wiped, leading to a data breach.

❓ **What is missing?** A Mobile Device Management (MDM) policy to

enforce security controls on all mobile devices accessing corporate resources.

💡 **How to fix?** Implement an MDM solution that enforces security measures such as device encryption, remote wiping, and access restrictions. Require mobile device users to enable password protection and multi-factor authentication (MFA). Establish policies governing acceptable use and define actions to take in case of lost or stolen devices.

39. Lack of privacy impact assessments

📌 **ISO 27001 Section: A.5.21 – Privacy & Data Protection**

🔍 **Scenario:** The organization collects and processes large amounts of personal data without conducting privacy impact assessments (PIAs). When a regulatory audit takes place, the company cannot demonstrate compliance with GDPR, leading to potential fines.

❓ **What is missing?** A structured process for evaluating privacy risks associated with data processing activities.

💡 **How to fix?** Integrate Privacy Impact Assessments (PIAs) into business operations to evaluate how data collection and processing may affect individuals' privacy. Conduct PIAs before implementing new technologies or launching data-driven projects. Maintain documentation to demonstrate compliance with privacy regulations.

40. No segregation of duties in critical processes

📌 **ISO 27001 Section: A.5.18 – Operational Security Controls**

🔍 **Scenario:** In the finance department, a single employee is responsible for both approving and processing payments. This lack of segregation allows fraudulent transactions to go undetected.

❓ **What is missing?** A segregation of duties (SoD) framework to minimize the risk of fraud and errors.
💡 **How to fix?** Establish a policy that enforces segregation of duties in key business processes. Ensure that high-risk tasks, such as financial transactions or user account management, require multi-level approval. Implement system-enforced controls to prevent conflicts of interest.

41. No emergency contact list for security incidents

📌 **ISO 27001 Section: A.5.24 – Incident Management**
🔍 **Scenario:** During a major cyberattack, employees are unsure whom to contact for immediate response. The organization does not have a documented emergency contact list for security incidents.
❓ **What is missing?** A predefined emergency response contact list to facilitate quick action during incidents.
💡 **How to fix?** Maintain an updated emergency contact list that includes security teams, senior management, and external incident response partners. Distribute the list to all employees and conduct periodic drills to ensure everyone knows their roles during a security incident.

42. Lack of formal data breach notification process

📌 **ISO 27001 Section: A.5.24 – Data Breach Handling**
🔍 **Scenario:** A data breach exposes customer records, but the organization fails to notify affected individuals and regulators within the required timeframe.
❓ **What is missing?** A documented data breach notification process to ensure timely disclosure of incidents.
💡 **How to fix?** Define and implement a breach response policy outlining

notification timelines, responsibilities, and procedures. Ensure compliance with applicable legal requirements, such as GDPR's 72-hour breach notification rule.

43. No procedure for handling security policy exceptions

📌 **ISO 27001 Section: A.5.31 – Policy Exception Management**

🔍 **Scenario:** An employee requests an exception to bypass a security policy for a legitimate business reason, but there is no formal process to review or approve exceptions. As a result, inconsistent and undocumented exceptions weaken security controls.

❓ **What is missing?** A policy exception handling framework to ensure that deviations are documented, justified, and controlled.

💡 **How to fix?** Establish a formal policy exception request and approval process. Define criteria for evaluating exceptions, assign accountability, and implement compensating controls when necessary. Maintain a record of all approved exceptions and conduct periodic reviews.

44. Weak physical access control to data centers

📌 **ISO 27001 Section: A.7.4 – Physical Security**

🔍 **Scenario:** Visitors and unauthorized personnel can access the data center without restrictions, increasing the risk of tampering and insider threats.

❓ **What is missing?** Strong access control mechanisms to protect critical infrastructure.

💡 **How to fix?** Implement multi-factor authentication, biometric security, and security guards for data center access. Require access approvals and maintain entry logs.

45. Lack of accountability for system administrators

📌 **ISO 27001 Section: A.8.2 – Privileged Access Management**
🔍 **Scenario:** System administrators have full access to IT infrastructure, but their activities are not logged or monitored. An insider threat goes undetected due to the lack of accountability measures.
❓ **What is missing?** A privileged access monitoring system to track and control administrator activities.
💡 **How to fix?** Implement privileged access management (PAM) solutions to monitor and log all administrator activities. Require approvals for high-risk actions and conduct periodic access reviews.

46. No encryption of backups

📌 **ISO 27001 Section: A.5.30 – Backup Security**
🔍 **Scenario:** The organization backs up sensitive data but does not encrypt the backups. A stolen or lost backup device exposes customer information, leading to potential regulatory fines.
❓ **What is missing?** Encryption for backup data to ensure confidentiality in case of data breaches or loss.
💡 **How to fix?** Implement strong encryption protocols for both cloud-based and physical backups. Use encryption keys securely stored in a hardware security module (HSM). Ensure backups are only accessible to authorized personnel and periodically test recovery procedures.

47. Inadequate monitoring of third-party access

📌 **ISO 27001 Section: A.5.19 – Supplier Access Control**
🔍 **Scenario:** Third-party vendors have remote access to the organization's network for system maintenance, but their activities are not logged or reviewed. A vendor account is compromised, leading to a data breach.
❓ **What is missing?** A monitoring system to track third-party access and activities within the organization's network.
💡 **How to fix?** Implement secure remote access solutions that require multi-factor authentication (MFA) for vendors. Set up monitoring tools to log third-party activities and generate alerts for suspicious actions. Periodically review access rights and remove unnecessary vendor permissions.

48. No security baseline for IT systems

📌 **ISO 27001 Section: A.5.13 – Secure System Configuration**
🔍 **Scenario:** IT systems are deployed with default configurations, including open ports and weak security settings. Attackers exploit these vulnerabilities to gain unauthorized access.
❓ **What is missing?** A security baseline configuration to ensure all IT systems follow best practices before deployment.
💡 **How to fix?** Develop and enforce security baseline configurations for all IT systems, ensuring they comply with security best practices. Regularly conduct configuration audits and use automated tools to detect deviations from the baseline.

49. Weak onboarding security processes

📌 **ISO 27001 Section: A.6.3 – Employee Security Awareness**
🔍 **Scenario:** New employees do not receive formal security training, leaving them unaware of company policies, phishing risks, and data protection requirements.
❓ **What is missing?** A structured onboarding security awareness program to educate employees from day one.
💡 **How to fix?** Develop a security induction program for all new hires, covering topics such as password security, phishing awareness, and acceptable use policies. Require employees to acknowledge security policies before gaining system access.

50. Failure to track legal and regulatory changes

📌 **ISO 27001 Section: A.5.31 – Compliance Monitoring**
🔍 **Scenario:** The organization is unaware of new data protection laws that impact its operations. A regulatory audit reveals non-compliance, leading to fines and legal action.
❓ **What is missing?** A compliance monitoring system to track evolving legal and regulatory requirements.
💡 **How to fix?** Establish a compliance tracking team responsible for monitoring changes in laws and regulations relevant to the business. Subscribe to regulatory updates, conduct periodic compliance reviews, and ensure policies and procedures are updated accordingly.

51. No documentation of security awareness training

📌 **ISO 27001 Section: A.6.3 – Awareness, Education, and Training**
🔍 **Scenario:** The company claims it conducts security training, but there is no documentation proving employee participation. An audit reveals gaps in training records.
❓ **What is missing?** A formal record-keeping system for security awareness training completion.
💡 **How to fix?** Implement a training management system to track attendance and completion rates for security awareness sessions. Require employees to acknowledge training completion and regularly update training materials to cover emerging threats.

52. No process for revoking third-party access

📌 **ISO 27001 Section: A.5.19 – Supplier Access Management**
🔍 **Scenario:** A vendor completes a contract but still has active access credentials to the organization's systems. This creates a security risk if the account is misused or compromised.
❓ **What is missing?** A formalized process to revoke third-party access when it is no longer needed.
💡 **How to fix?** Implement an access revocation procedure that ensures vendor accounts are deactivated immediately upon contract completion. Automate the process using identity and access management (IAM) tools.

53. Weak security for cloud-based applications

📌 **ISO 27001 Section: A.5.22 – Cloud Security Controls**
🔍 **Scenario:** Employees use cloud-based applications to store and share corporate data without encryption or access controls. A misconfigured cloud bucket leads to a data leak.
❓ **What is missing?** Security policies and controls for protecting cloud-based applications and data.
💡 **How to fix?** Enforce cloud security best practices, including encryption, access control, and logging. Use Cloud Access Security Brokers (CASBs) to monitor cloud application usage and enforce compliance.

54. No logging of privileged user activities

📌 **ISO 27001 Section: A.8.2 – Privileged Account Monitoring**
🔍 **Scenario:** System administrators perform high-privilege actions without accountability. A misconfiguration leads to downtime, but no logs exist to determine the cause.
❓ **What is missing?** Logging and monitoring of privileged user activities to ensure accountability.
💡 **How to fix?** Implement privileged session monitoring and logging solutions. Enforce least-privilege principles and regularly review logs for suspicious activity.

55. Lack of asset tracking and tagging

📌 **ISO 27001 Section: A.5.9 – Asset Management**
🔍 **Scenario:** IT equipment is frequently lost or misplaced, leading to data

security risks. The organization lacks a structured process to track and tag assets.

❓ **What is missing?** A comprehensive asset tracking and management system.

💡 **How to fix?** Deploy an asset management system that maintains an up-to-date inventory of hardware and software. Use asset tags and tracking tools to prevent unauthorized removal of critical assets.

56. No regular security policy reviews

📌 **ISO 27001 Section: A.5.31 – Security Policy Review**

🔍 **Scenario:** Security policies were created years ago and have not been updated, leading to outdated guidelines that do not address modern threats.

❓ **What is missing?** A structured review process for security policies.

💡 **How to fix?** Establish an annual policy review cycle to update security policies based on new threats, regulatory changes, and business needs.

57. No defined incident response playbooks

📌 **ISO 27001 Section: A.5.24 – Incident Response Management**

🔍 **Scenario:** Employees do not know how to respond to a cyberattack, leading to confusion and delays in containment.

❓ **What is missing?** Predefined incident response playbooks for handling different types of security incidents.

💡 **How to fix?** Develop and document incident response playbooks for various scenarios (e.g., ransomware, phishing, data breaches). Conduct regular incident response drills.

58. No clear guidelines for handling sensitive data

📌 **ISO 27001 Section: A.5.12 – Data Protection & Handling**

🔍 **Scenario:** Employees frequently email sensitive customer information without encryption or store confidential data on shared drives with unrestricted access. An external audit reveals numerous policy violations, exposing the organization to compliance risks.

❓ **What is missing?** Clear guidelines and policies on handling, transmitting, and storing sensitive data securely.

💡 **How to fix?** Develop and enforce a data handling policy specifying encryption requirements, access control measures, and data-sharing restrictions. Conduct regular training sessions to educate employees on handling sensitive information securely and monitor adherence through compliance audits.

59. No regular penetration testing schedule

📌 **ISO 27001 Section: A.5.25 – Vulnerability Assessment & Testing**

🔍 **Scenario:** The organization performs ad-hoc penetration testing only after major security incidents. As a result, vulnerabilities in web applications and network infrastructure remain undetected, exposing the organization to potential cyberattacks.

❓ **What is missing?** A formalized and regular penetration testing schedule to proactively identify and mitigate security weaknesses.

💡 **How to fix?** Implement a structured penetration testing program that includes internal and external tests at least annually. Engage certified ethical hackers to simulate attacks and document vulnerabilities. Prioritize

and remediate identified weaknesses as part of an ongoing security improvement plan.

60. No policy for removable media usage

📌 **ISO 27001 Section: A.5.14 – Removable Media Security**
🔍 **Scenario:** Employees frequently use USB drives, external hard disks, and SD cards to transfer corporate data without security controls. A lost unencrypted USB drive containing customer data leads to a regulatory investigation.
❓ **What is missing?** A strict removable media policy that defines security measures for portable storage devices.
💡 **How to fix?** Restrict the use of removable media through policy enforcement and endpoint security controls. Require encryption for all portable devices containing sensitive data. Educate employees on the risks of using unauthorized media and enforce logging of removable device access.

61. No review process for access permissions

📌 **ISO 27001 Section: A.8.2 – User Access Review**
🔍 **Scenario:** Employees who have changed roles within the company retain access to systems they no longer require. A recent security audit reveals that former contractors still have active accounts, posing a security risk.
❓ **What is missing?** A structured access review process to ensure that only authorized individuals have access to critical systems.
💡 **How to fix?** Implement a periodic access review process, requiring system owners to verify user permissions and remove outdated accounts.

Enforce role-based access control (RBAC) to automatically adjust access rights based on job responsibilities.

62. Lack of incident response time objectives

📌 **ISO 27001 Section: A.5.24 – Incident Response Management**
🔍 **Scenario:** During a cybersecurity breach, the IT team takes hours to respond due to unclear guidelines on response timelines. The delay results in prolonged downtime and increased data exposure.
❓ **What is missing?** Defined incident response time objectives (RTOs) and response procedures to minimize damage and downtime.
💡 **How to fix?** Establish predefined incident response time objectives and classify incidents by severity. Implement an incident response framework that includes predefined playbooks for different types of security incidents. Conduct tabletop exercises to test response effectiveness.

63. No endpoint detection and response (EDR) solution

📌 **ISO 27001 Section: A.5.27 – Security Monitoring**
🔍 **Scenario:** The organization relies solely on traditional antivirus software for malware detection. A sophisticated ransomware attack bypasses signature-based detection, encrypting critical files and halting business operations.
❓ **What is missing?** Advanced endpoint security controls to detect and respond to modern cyber threats.
💡 **How to fix?** Deploy an endpoint detection and response (EDR) solution that provides real-time monitoring, threat hunting, and automated remediation. Integrate EDR with a Security Information and Event Management (SIEM) system for centralized security visibility.

64. No secure file-sharing policy

📌 **ISO 27001 Section: A.5.22 – Cloud & File-Sharing Security**
🔍 **Scenario:** Employees use third-party file-sharing services (e.g., Google Drive, Dropbox) to transfer corporate documents without security oversight. A misconfigured folder allows unauthorized external users to access internal documents.
❓ **What is missing?** A secure file-sharing policy to ensure data security and compliance with corporate security policies.
💡 **How to fix?** Establish a secure file-sharing policy that mandates the use of approved platforms with encryption and access controls. Implement logging and monitoring of file-sharing activities and educate employees on secure data transfer best practices.

65. No policy for decommissioning IT assets

📌 **ISO 27001 Section: A.5.9 – Asset Management**
🔍 **Scenario:** Old servers and laptops are discarded without secure data wiping, leading to a data leak when a third party retrieves an old hard drive containing sensitive customer information.
❓ **What is missing?** A decommissioning policy that ensures proper disposal of retired IT assets to prevent unauthorized access to sensitive data.
💡 **How to fix?** Implement a structured IT asset disposal policy that includes secure wiping, physical destruction, or certified e-waste disposal. Maintain logs of all decommissioned devices and verify disposal methods for compliance.

66. No policy for handling insider threats

📌 **ISO 27001 Section: A.5.18 – Insider Threat Management**
🔍 **Scenario:** A disgruntled employee downloads sensitive company data before resigning and shares it with a competitor. The company has no monitoring or prevention mechanisms in place to detect and stop insider threats.
❓ **What is missing?** A policy for identifying, monitoring, and mitigating risks associated with insider threats.
💡 **How to fix?** Implement behavioral analytics and user activity monitoring tools to detect suspicious actions. Establish an insider threat response program that includes access revocation for departing employees and policies for reporting suspicious behavior.

67. No multifactor authentication (MFA) enforcement

📌 **ISO 27001 Section: A.8.3 – Secure Authentication**
🔍 **Scenario:** Employees access critical business applications using only a username and password. A phishing attack compromises credentials, leading to unauthorized access to financial records.
❓ **What is missing?** Enforced multifactor authentication (MFA) to enhance authentication security.
💡 **How to fix?** Require MFA for all critical applications and remote access. Use a combination of authentication factors such as biometrics, hardware tokens, and time-based one-time passwords (TOTPs).

68. No audit trails for financial transactions

📌 **ISO 27001 Section: A.5.31 – Financial Security Monitoring**
🔍 **Scenario:** A finance department employee manipulates transaction records to commit fraud. The organization lacks audit trails, making it difficult to trace and investigate unauthorized financial activities.
❓ **What is missing?** Detailed audit logs for all financial transactions to ensure accountability and fraud detection.
💡 **How to fix?** Implement financial system logging to track all transaction activities. Regularly review logs and set up alerts for anomalies, ensuring compliance with financial security regulations.

69. No defined process for revoking privileged access

📌 **ISO 27001 Section: A.8.2 – Privileged Access Management**
🔍 **Scenario:** A system administrator who recently changed roles retains full administrative access, leading to unauthorized changes.
❓ **What is missing?** A structured process for revoking privileged access when job roles change.
💡 **How to fix?** Establish a privileged access management (PAM) system that automatically revokes administrative rights when no longer needed. Conduct periodic privilege reviews.

70. No monitoring of privileged user activities

📌 **ISO 27001 Section: A.8.2 – Privileged Access Management**
🔍 **Scenario:** The organization grants system administrators unrestricted access to critical IT infrastructure. However, there is no monitoring or

logging of their activities, allowing potential misuse of privileges to go undetected. A system administrator makes unauthorized changes to the firewall settings, exposing the network to external threats, but no logs are available to trace the action.

❓ **What is missing?** A robust monitoring and auditing process for privileged user activities to ensure accountability.

💡 **How to fix?** Implement Privileged Access Management (PAM) solutions to monitor and log all privileged user activities. Enforce multi-factor authentication (MFA) for administrator accounts and review logs regularly for anomalies. Conduct periodic audits to ensure privileged users adhere to security policies.

71. No policy for managing inactive user accounts

📌 **ISO 27001 Section: A.8.2 – Identity and Access Management**

🔍 **Scenario:** The IT department does not regularly review inactive user accounts. As a result, accounts belonging to former employees and contractors remain active for months, creating a security risk. A cybercriminal exploits one of these dormant accounts to gain unauthorized access to the network.

❓ **What is missing?** A policy for identifying and disabling inactive user accounts.

💡 **How to fix?** Implement an automated process to deactivate inactive accounts after a predefined period. Conduct periodic reviews of all user accounts to identify and remove unused accounts. Require managers to validate employee access during offboarding to ensure timely deactivation.

72. No restrictions on administrative access to end-user devices

📌 **ISO 27001 Section: A.8.2 – Least Privilege Access**
🔍 **Scenario:** Employees have administrative privileges on their work laptops, allowing them to install unauthorized applications. Malware is introduced into the corporate network when an employee unknowingly downloads a malicious application.
❓ **What is missing?** Restrictions on administrative privileges to reduce security risks associated with unauthorized installations.
💡 **How to fix?** Implement the principle of least privilege by restricting administrative access to IT personnel only. Use endpoint security solutions to enforce application whitelisting and prevent unauthorized software installations. Regularly audit user privileges to ensure compliance.

73. No protection against brute-force attacks

📌 **ISO 27001 Section: A.8.3 – Authentication Security**
🔍 **Scenario:** The organization does not have an account lockout policy in place, allowing unlimited login attempts. Attackers use automated tools to repeatedly guess employee passwords, eventually gaining access to sensitive data.
❓ **What is missing?** Security controls to prevent brute-force attacks on authentication systems.
💡 **How to fix?** Implement an account lockout mechanism that temporarily disables accounts after multiple failed login attempts. Enforce strong password policies and require multi-factor authentication (MFA) for all critical systems. Deploy intrusion detection systems (IDS) to detect and block brute-force attempts.

74. No centralized logging and event correlation

📌 **ISO 27001 Section: A.5.27 – Security Monitoring**
🔍 **Scenario:** Security logs are scattered across different servers and applications, making it difficult to detect suspicious activities. A cyberattack goes unnoticed for weeks because no centralized monitoring system exists.
❓ **What is missing?** A centralized logging and event correlation system to detect and respond to security incidents efficiently.
💡 **How to fix?** Implement a Security Information and Event Management (SIEM) system to aggregate and analyze logs in real time. Configure alerts for anomalous activities and integrate logs from network devices, endpoints, and cloud applications. Conduct periodic log reviews to identify potential security incidents.

75. No security awareness testing for employees

📌 **ISO 27001 Section: A.6.3 – Security Awareness and Training**
🔍 **Scenario:** Employees complete annual security training but are never tested on their knowledge. When a phishing attack occurs, multiple employees fall victim, revealing their login credentials to attackers.
❓ **What is missing?** Regular security awareness testing to evaluate employee understanding and preparedness.
💡 **How to fix?** Conduct simulated phishing attacks and social engineering tests to measure employee awareness. Use quiz-based assessments to reinforce learning and track progress over time. Provide targeted training to employees who fail security awareness tests.

76. No formal process for handling third-party security assessments

📌 **ISO 27001 Section: A.5.19 – Supplier Security Management**
🔍 **Scenario:** The organization relies on third-party vendors for critical services but does not assess their security controls. A vendor experiences a data breach, exposing the organization's customer data, but there was no prior evaluation of their security posture.
❓ **What is missing?** A formalized process for assessing and monitoring the security posture of third-party vendors.
💡 **How to fix?** Develop a third-party security assessment framework that requires vendors to complete security questionnaires, provide compliance certifications, and undergo audits before engaging in business. Establish contractual obligations for security compliance and periodic reassessments.

77. No policy for handling abandoned workstations

📌 **ISO 27001 Section: A.7.4 – Physical Security**
🔍 **Scenario:** Employees frequently leave their workstations unattended without locking their screens. An unauthorized individual gains access to a logged-in workstation and retrieves confidential data.
❓ **What is missing?** A policy to prevent unauthorized access to unattended workstations.
💡 **How to fix?** Implement an automatic screen lock policy that locks devices after a short period of inactivity. Educate employees on the importance of locking their screens when stepping away. Conduct periodic security audits to enforce compliance.

78. No periodic review of security policies

📌 **ISO 27001 Section: A.5.31 – Policy Management**

🔍 **Scenario:** The organization's security policies were last updated three years ago and do not reflect current threats or regulatory changes. Employees continue following outdated procedures, exposing the organization to compliance risks.

❓ **What is missing?** A structured process for reviewing and updating security policies.

💡 **How to fix?** Establish an annual review process for security policies to ensure alignment with evolving threats, technologies, and regulations. Assign responsibility to a dedicated security team to track policy updates and communicate changes to employees.

79. No process for removing temporary accounts

📌 **ISO 27001 Section: A.8.2 – Access Management**

🔍 **Scenario:** The IT department creates temporary accounts for contractors and short-term employees but fails to deactivate them once the contract ends. Attackers compromise an unused temporary account to gain access to internal systems.

❓ **What is missing?** A process to systematically disable temporary accounts after their intended use.

💡 **How to fix?** Implement an automated account expiration system that disables temporary accounts after a predefined period. Require periodic reviews of active accounts to ensure temporary credentials are removed promptly.

80. No policy for securing IoT devices

📌 **ISO 27001 Section: A.5.22 – Internet of Things (IoT) Security**
🔍 **Scenario:** The organization deploys IoT devices such as smart cameras and sensors but does not implement security controls. Default passwords remain unchanged, allowing attackers to gain remote access and spy on internal operations.
❓ **What is missing?** A security policy addressing the risks associated with IoT devices.
💡 **How to fix?** Implement a dedicated IoT security policy that requires device authentication, encryption, and network segmentation. Change default credentials before deployment and apply firmware updates regularly to patch vulnerabilities.

81. No defined process for revoking physical access

📌 **ISO 27001 Section: A.7.4 – Physical Security**
🔍 **Scenario:** Employees and contractors who no longer work for the organization still have active access cards, allowing them to enter secure areas such as server rooms. A former employee enters the office unnoticed and removes sensitive documents.
❓ **What is missing?** A structured process to revoke physical access when an employee or contractor leaves the organization.
💡 **How to fix?** Implement an automated system for disabling access cards and collecting physical keys upon termination. Conduct periodic audits of access logs to identify unauthorized attempts and enforce compliance with physical security policies.

82. No policy for securing home offices in remote work setups

📌 **ISO 27001 Section: A.6.3 – Remote Work Security**
🔍 **Scenario:** Employees working remotely do not follow security best practices. Confidential client data is printed at home and left in open areas. Personal devices without endpoint protection are used to access corporate systems.
❓ **What is missing?** A policy that defines security measures for home offices to prevent unauthorized data exposure.
💡 **How to fix?** Establish a remote work security policy that requires encrypted VPN access, endpoint protection, and secure document disposal methods. Provide employees with secure corporate devices and mandate security training for remote work environments.

83. No formal data classification training for employees

📌 **ISO 27001 Section: A.5.10 – Data Classification & Handling**
🔍 **Scenario:** Employees do not understand the classification levels of data and often mishandle confidential information. Internal reports labeled "confidential" are shared with third parties without encryption.
❓ **What is missing?** Training on data classification and handling best practices.
💡 **How to fix?** Conduct periodic training on data classification policies. Implement tools that automatically label and enforce protection controls based on data classification. Ensure employees understand the implications of mishandling sensitive data.

84. No process for securely disposing of printed sensitive documents

📌 **ISO 27001 Section: A.5.12 – Secure Document Disposal**
🔍 **Scenario:** Confidential printed reports are thrown into regular trash bins instead of being shredded. A competitor retrieves and uses these discarded documents to gain a business advantage.
❓ **What is missing?** A secure document disposal process to ensure that sensitive information is permanently destroyed.
💡 **How to fix?** Implement shredding policies for all confidential documents and place secure disposal bins in office areas. Use third-party document destruction services that provide a certificate of disposal. Train employees on the importance of secure document disposal.

85. No security policy enforcement for third-party integrations

📌 **ISO 27001 Section: A.5.19 – Supplier & Third-Party Security**
🔍 **Scenario:** The organization integrates third-party applications into its systems without verifying their security posture. A vulnerable third-party tool is exploited, leading to unauthorized access to internal databases.
❓ **What is missing?** A policy to enforce security assessments before integrating third-party applications.
💡 **How to fix?** Establish a third-party risk assessment process that evaluates vendors before allowing integrations. Require security certifications, penetration testing reports, and compliance audits from third parties. Use secure APIs with authentication and encryption for all integrations.

86. No security validation before launching new software

📌 **ISO 27001 Section: A.5.33 – Secure Development**
🔍 **Scenario:** A new customer portal is launched without conducting security testing. Within days, attackers exploit SQL injection vulnerabilities, leading to customer data leakage.
❓ **What is missing?** A security validation process in the software development lifecycle (SDLC).
💡 **How to fix?** Implement security testing as a mandatory step before launching any software. Conduct code reviews, static and dynamic analysis, and penetration testing. Establish a DevSecOps framework to integrate security from the early stages of development.

87. No protection against insider fraud

📌 **ISO 27001 Section: A.5.18 – Fraud Prevention**
🔍 **Scenario:** A finance employee manipulates vendor invoices to embezzle company funds. Weak internal controls allow fraudulent transactions to go unnoticed for months.
❓ **What is missing?** Anti-fraud measures, such as segregation of duties and monitoring financial transactions.
💡 **How to fix?** Implement internal financial controls that require dual approval for transactions above a certain threshold. Conduct fraud awareness training and implement behavior analytics to detect suspicious activities.

88. No incident recovery testing

📌 **ISO 27001 Section: A.5.28 – Business Continuity & Disaster Recovery**

🔍 **Scenario:** After a ransomware attack, IT staff attempts to restore backups, only to find that the backup files are corrupt and unusable. The organization is unable to recover critical business data.

❓ **What is missing?** Regular testing of incident recovery procedures to ensure data and system restoration effectiveness.

💡 **How to fix?** Conduct scheduled backup restoration tests and ensure redundancy with offsite or cloud-based backups. Develop an incident recovery playbook and train teams on recovery procedures.

89. No policy for detecting and preventing unauthorized network devices

📌 **ISO 27001 Section: A.5.17 – Network Security**

🔍 **Scenario:** Employees connect unauthorized personal routers and IoT devices to the corporate network, creating security risks. IT is unaware of these rogue devices, which could be exploited by attackers.

❓ **What is missing?** Network monitoring and access control measures to detect and prevent unauthorized devices.

💡 **How to fix?** Deploy Network Access Control (NAC) solutions to enforce device authentication. Regularly scan the network for unknown devices and block unapproved hardware.

90. No employee security performance evaluation

📌 **ISO 27001 Section: A.6.3 – Security Awareness & Performance**
🔍 **Scenario:** Employees undergo security training but their adherence to security policies is never assessed. Those who continuously fail phishing simulations face no corrective actions.
❓ **What is missing?** A mechanism to evaluate employee security performance and enforce accountability.
💡 **How to fix?** Implement a security performance scorecard that tracks employee adherence to policies, incident reporting participation, and security test results. Provide additional training for employees with poor security behavior.

91. No multi-cloud security strategy

📌 **ISO 27001 Section: A.5.22 – Cloud Security Management**
🔍 **Scenario:** The organization uses multiple cloud service providers (AWS, Azure, and Google Cloud) but does not have a unified security policy. Security configurations vary across platforms, leading to inconsistent access controls and misconfigurations that expose sensitive data.
❓ **What is missing?** A standardized multi-cloud security strategy to ensure security controls are consistently applied across cloud environments.
💡 **How to fix?** Implement a Cloud Security Posture Management (CSPM) tool to monitor and enforce security compliance across multiple cloud platforms. Define a multi-cloud security strategy that standardizes access control, encryption policies, and network configurations. Conduct regular cloud security assessments to detect misconfigurations.

92. No policy for Bring Your Own Device (BYOD) applications

📌 **ISO 27001 Section: A.5.15 – Mobile Device Security**
🔍 **Scenario:** Employees install unauthorized applications on their personal devices used for work, increasing the risk of data leaks and malware infections. A mobile device used for corporate email is compromised due to a third-party app with hidden malware.
❓ **What is missing?** A Bring Your Own Device (BYOD) policy that governs the use of applications on personal devices accessing corporate resources.
💡 **How to fix?** Enforce Mobile Device Management (MDM) policies that restrict the installation of unapproved applications on work-related personal devices. Require employees to use a secure corporate container for business applications and enforce encryption on mobile devices. Educate employees on the risks of untrusted apps and enforce regular security updates.

93. No automated patch deployment

📌 **ISO 27001 Section: A.5.23 – Patch Management**
🔍 **Scenario:** The IT department manually deploys software patches, leading to delays in updating critical systems. A known vulnerability in an outdated web application remains unpatched for months, allowing attackers to exploit it and gain access to sensitive customer records.
❓ **What is missing?** An automated patch management system to ensure timely deployment of security updates.
💡 **How to fix?** Implement an automated patch management system that monitors, downloads, and applies patches without manual intervention. Configure systems to deploy critical security updates immediately while testing non-critical updates before deployment. Conduct periodic vulnerability assessments to identify unpatched software.

94. No policy for external media scanning

📌 **ISO 27001 Section: A.5.14 – External Media Control**

🔍 **Scenario:** Employees frequently use USB drives and external hard disks without any security scanning. An infected USB drive containing ransomware is plugged into a corporate laptop, leading to a widespread network infection.

❓ **What is missing?** A policy requiring external media to be scanned for malware before use.

💡 **How to fix?** Enforce an external media security policy that mandates automatic malware scanning of all external storage devices before they can be accessed. Disable USB ports on corporate devices unless explicitly approved. Use endpoint security solutions to monitor and control external media usage.

95. No monitoring of social engineering attempts

📌 **ISO 27001 Section: A.5.24 – Social Engineering Protection**

🔍 **Scenario:** Employees receive fake phone calls from attackers impersonating IT support. Without verification, they unknowingly provide their login credentials, leading to an account compromise. There is no mechanism in place to detect and report such incidents.

❓ **What is missing?** A structured process to detect and mitigate social engineering attempts.

💡 **How to fix?** Conduct simulated social engineering attacks (e.g., phishing, vishing) to test employee awareness. Implement an employee verification system for all IT support-related requests. Create an incident response

protocol to track and analyze social engineering attempts and educate employees on recognizing scams.

96. No redundancy for internet connectivity

📌 **ISO 27001 Section: A.5.28 – Business Continuity and Redundancy**
🔍 **Scenario:** The organization relies on a single internet service provider (ISP) for connectivity. A prolonged outage due to ISP failure halts business operations, preventing employees from accessing cloud services.
❓ **What is missing?** Redundant internet connectivity to ensure business continuity during ISP failures.
💡 **How to fix?** Establish multiple ISP connections with automatic failover capabilities. Use software-defined wide area networking (SD-WAN) to manage internet traffic dynamically and ensure continuous connectivity. Regularly test failover mechanisms to confirm operational effectiveness.

97. No restrictions on file-sharing permissions

📌 **ISO 27001 Section: A.5.10 – Access Control for Shared Data**
🔍 **Scenario:** Employees store sensitive files on shared drives with unrestricted access. An intern accidentally deletes critical files, and another unauthorized employee gains access to payroll information.
❓ **What is missing?** Proper access control mechanisms to prevent unauthorized access to shared files.
💡 **How to fix?** Implement role-based access control (RBAC) for shared file storage to restrict access based on user roles. Enforce read-only permissions for non-editing users. Enable logging to track file access and modifications.

98. No audit process for software licenses

📌 **ISO 27001 Section: A.5.31 – Software Compliance**
🔍 **Scenario:** Employees install unlicensed software on company devices, violating compliance regulations. The organization is audited and fined for using pirated software.
❓ **What is missing?** A software license audit process to ensure compliance with legal and contractual requirements.
💡 **How to fix?** Implement a Software Asset Management (SAM) program to track all software installations. Conduct periodic software license audits and enforce policies that restrict unauthorized software installations.

99. No compliance tracking for regulatory changes

📌 **ISO 27001 Section: A.5.31 – Regulatory Compliance Management**
🔍 **Scenario:** The organization is unaware of new data privacy laws affecting its operations. A regulatory audit reveals non-compliance, leading to financial penalties.
❓ **What is missing?** A system for tracking and implementing changes in compliance regulations.
💡 **How to fix?** Establish a compliance tracking team responsible for monitoring legal and regulatory updates. Subscribe to industry bulletins and legal advisories. Ensure that security policies and practices are updated in alignment with new compliance requirements.

100. No process for reporting security concerns anonymously

📌 **ISO 27001 Section: A.5.24 – Incident Reporting and Whistleblower Protection**

🔍 **Scenario:** Employees witness security vulnerabilities and policy violations but do not report them due to fear of retaliation. As a result, critical security gaps remain undetected.

❓ **What is missing?** A secure and anonymous reporting mechanism for employees to raise security concerns.

💡 **How to fix?** Implement a whistleblower policy that ensures anonymity for individuals reporting security concerns. Provide multiple channels for reporting, such as an anonymous online form or encrypted email system. Promote a security-conscious culture where employees feel encouraged to report threats without fear of consequences.

Strengthening Your ISO 27001 Compliance Journey

Achieving and maintaining ISO 27001 compliance is not just about passing an audit—it's about building a strong, resilient, and secure organization.

By addressing these 100 common non-conformities, you are not only improving compliance but also enhancing your overall cybersecurity posture and minimizing risks that could lead to costly security incidents.

🔷 **Continuous Improvement is Key –** Compliance is an ongoing process. Regular audits, employee training, and security assessments will help keep your ISMS effective and aligned with evolving threats.

🔷 **Documentation and Accountability Matter** – Keep detailed records of your security policies, risk assessments, and corrective actions to demonstrate your commitment to ISO 27001 standards.

🔷 **Turn Compliance Into a Competitive Advantage** – A well-implemented ISMS not only ensures security but also builds trust with clients, partners, and regulators, making your organization more competitive in the marketplace.

Use this guide as a practical roadmap to identify security gaps, implement necessary fixes, and maintain an ISO 27001-compliant environment. Stay proactive, stay secure, and let compliance drive business success!

GSDC
Global Skill Development Council

CERTIFIED ISO 27001:2022 LEAD AUDITOR

ISO 27001 Lead Auditor Certification is based on Information Security Management Systems.

ABOUT GSDC CERTIFICATION

LIFETIME VALIDITY

GSDC Certification is an globally accreditted certification with lifetime validity.

EBOOK

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

CREATED BY EXPERTS

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

LEARNING MATERIALS

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

LEARNING OBJECTIVE

- **Evaluate the effectiveness of ISMS.**
- **Conduct thorough audits of security controls**
- **Promote confidentiality, integrity, and availability.**
- **Develop proficiency through ISO 27001 training**

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

Enroll Now

www.gsdcouncil.org