

GAQM ISO-CLA-22

GAQM ISO / IEC 27002 - Lead Implementer

**Thank You for Downloading ISO-CLA-22 Updated Exam
Questions**

<https://certs4sale.com/gaqm/iso-cla-22-pdf-exam-dumps>

QUESTION: 1

Imagine a significant data breach occurs after an ISO 27001 certification audit. The auditor's report stated no major nonconformities regarding access controls. Which action is MOST appropriate for the certified organization immediately?

Option A : Ignore the breach as the organization is already certified and a subsequent audit will address it.

Option B : Immediately notify the certification body (CB) of the breach and initiate a thorough investigation to determine if there were any systemic failures not identified during the audit.

Option C : Issue a press release stating the organization is ISO 27001 certified, therefore, the breach was likely an external attack and not an internal control failure.

Option D : Wait for the next surveillance audit to inform the CB about the breach and any corrective actions taken.

Correct Answer: B

Explanation/Reference:

The MOST appropriate action is to immediately notify the certification body and initiate a thorough investigation. This demonstrates transparency, allows for a proper assessment of the breach's impact on the ISMS and certification, and allows the organization to take corrective actions promptly. Ignoring the breach or delaying notification could invalidate the certification and undermine the organization's security posture. The fact that the organization is certified doesn't excuse the need to address the breach thoroughly.

QUESTION: 2

Prior to conducting a Stage 2 audit for ISO/IEC 27001 certification, what's the MOST important objective a Lead Auditor should prioritize to ensure a comprehensive and efficient assessment?

Option A : Confirm all identified nonconformities from the Stage 1 audit have been fully addressed and closed with verifiable evidence.

Option B : Thoroughly review the Statement of Applicability (SoA) to ensure all necessary controls are implemented and aligned with the organization's risk assessment.

Option C : Conduct a detailed review of the organization's business continuity plan (BCP) to ensure its effectiveness in addressing potential disruptions.

Option D : Ensure the audit team possesses the necessary technical expertise and resources to effectively evaluate the organization's information security management system (ISMS).

Correct Answer: C

Explanation/Reference:

The MOST important objective prior to a Stage 2 audit is to thoroughly review the Statement of Applicability (SoA). The SoA outlines the controls implemented by the organization and their justification for inclusion or exclusion. Assessing the SoA thoroughly ensures that the Stage 2 audit focuses on the areas of the ISMS that are most relevant to the organization's specific risks and objectives, confirming that the scope of the ISMS is well-defined and correctly executed. Without a complete and accurate SoA the whole implementation cannot be properly evaluated.

QUESTION: 3

Focusing internal audit, which aspect of the documented audit program is MOST crucial for ensuring objective evidence of continuous improvement within the ISMS?

- Option A : The detailed itinerary of each auditor's activities during the audit.
- Option B : The established criteria for selecting specific controls for testing during the audit.
- Option C : The defined process for handling nonconformities identified during the audit.
- Option D : The record of management review meetings following each audit cycle discussing audit findings and corrective actions.

Correct Answer: D

Explanation/Reference:

The most crucial aspect for proving continuous improvement isn't just identifying problems (nonconformities) or selecting controls for testing; it's demonstrably taking action based on audit findings and showing that the ISMS is evolving and becoming more effective over time. Documented management review meetings which discusses audit findings and subsequent corrective actions are key to meeting the requirements for ongoing improvement in an ISMS. Hence option 4 is the most appropriate response.

QUESTION: 4

Suppose a lead auditor observes that a minor nonconformity, initially raised during the audit, has been addressed by the auditee with documented corrective action verified as effective during the closing meeting. However, the evidence was submitted just before the meeting started. What is the MOST appropriate action for the lead auditor?

- Option A : Immediately close the nonconformity and proceed with a recommendation for certification.

Option B : Document the closure of the nonconformity in the audit report and recommend certification, highlighting the last-minute evidence submission.

Option C : Insist on scheduling a follow-up audit to independently verify the corrective action's long-term effectiveness before recommending certification.

Option D : Note the closure and recommend certification but stipulate that the next surveillance audit must specifically focus on the sustained effectiveness of this corrective action.

Correct Answer: D

Explanation/Reference:

The most appropriate action is to recommend certification but stipulate focused attention on the area during the next surveillance audit. This acknowledges the corrective action taken, addresses the auditor's concerns about the late evidence submission, and ensures ongoing effectiveness is verified in the future. It's a practical and reasonable approach in line with ISO/IEC 27001 auditing principles.

QUESTION: 5

Considering resource allocation, which activity MOST significantly impacts the effectiveness of the audit program when managing multiple ISO/IEC 27001 audits across different departments with varying risk profiles?

Option A : Providing generic checklists applicable to all departments to ensure consistency.

Option B : Allocating auditor time and expertise proportionally to the risk profile and complexity of each department's ISMS.

Option C : Scheduling all departmental audits consecutively to minimize travel expenses for the audit team.

Option D : Using only internal auditors to reduce external audit costs and maintain confidentiality.

Correct Answer: B

Explanation/Reference:

The effectiveness of an audit program hinges on properly allocating resources based on the assessed risk. Option 2, allocating auditor time and expertise proportionally to the risk profile and complexity of each department's ISMS, is the most significant activity. This approach ensures that high-risk areas receive appropriate attention, maximizing the value and impact of the audits. The other options prioritize cost savings or consistency over effectiveness, potentially overlooking critical vulnerabilities.

QUESTION: 6

Following audit confirmation, what principle is MOST directly threatened when the auditee's department head, who is also a personal friend of the Lead Auditor, is responsible for providing all documentation and coordinating all interviews for that department's processes?

- Option A : Fair Presentation
- Option B : Due Professional Care
- Option C : Integrity
- Option D : Independence

Correct Answer: D

Explanation/Reference:

The principle of Independence is most directly threatened. The auditee's department head's control over documentation and interviews, combined with their personal relationship with the Lead Auditor, creates a conflict of interest and undermines the auditor's objectivity. While integrity and fair presentation are important principles, the lack of independence has the most immediate and significant impact on the audit's validity.

QUESTION: 7

Inherent risks identification, associated with ISMS asset valuation, plays a crucial role in determining information security controls. Which statement MOST accurately reflects the impact of accurately identifying inherent risks on the ISMS?

- Option A : It primarily helps in selecting the most cost-effective security controls, regardless of the potential impact on data confidentiality.
- Option B : It facilitates the development of a comprehensive risk treatment plan, enabling the organization to prioritize and address vulnerabilities based on their potential impact and likelihood.
- Option C : It allows the organization to completely eliminate all potential information security threats, ensuring a secure environment.
- Option D : It mainly focuses on ensuring compliance with legal requirements, regardless of the actual risks the organization faces.

Correct Answer: B

Explanation/Reference:

Accurate identification of inherent risks is crucial for developing an effective ISMS. This allows the organization to

prioritize and address vulnerabilities based on their potential impact and likelihood. Selecting the most cost-effective security controls and ensuring compliance are related but subordinate to the primary goal of managing inherent risk and facilitating the development of a comprehensive risk treatment plan.

QUESTION: 8

Assuming multiple minor nonconformities are identified during Stage 2 audit of an organization seeking ISO/IEC 27001 certification, and management demonstrates a credible plan for corrective action, what's the auditor's MOST appropriate next step?

Option A : Immediately recommend certification withdrawal due to the presence of nonconformities.

Option B : Issue a conditional recommendation for certification, contingent upon successful implementation of the corrective action plan within a defined timeframe.

Option C : Delay the certification recommendation until a follow-up audit confirms complete closure of all minor nonconformities.

Option D : Recommend full certification, as minor nonconformities do not inherently preclude certification if a corrective action plan is in place.

Correct Answer: B

Explanation/Reference:

A conditional recommendation is the most appropriate action. It acknowledges the identified minor nonconformities and the organization's commitment to address them through a corrective action plan. This approach aligns with the principles of continuous improvement and allows for certification with the understanding that the nonconformities must be resolved and verified within a specified timeframe to maintain certification. It balances the need for compliance with the recognition of the organization's effort towards improvement. Full certification isn't appropriate as the nonconformities exist. Immediate withdrawal or complete delay are both too extreme given the circumstances.

QUESTION: 9

What key decision must the audit team make during the closing meeting when presented with conflicting evidence regarding a minor nonconformity's severity?

Option A : Escalate the issue directly to the certification body for immediate arbitration.

Option B : Delay the closing meeting indefinitely while gathering additional evidence to resolve the conflict internally.

Option C : The Lead Auditor must make a judgment call based on the preponderance of evidence and document the rationale.

Option D : Automatically classify the finding as a major nonconformity to err on the side of caution and ensure improvement.

Correct Answer: C

Explanation/Reference:

During the closing meeting, conflicting evidence sometimes arises. The Lead Auditor must use their expertise to weigh the available evidence, consider the impact on the ISMS, and make a reasoned judgment about the severity of the nonconformity. The rationale for this decision must be clearly documented to maintain transparency and audit trail integrity. Arbitrarily escalating or delaying the closing is not appropriate; a professional, balanced assessment is required.

QUESTION: 10

Understanding nonconformity categorization, which level signifies a significant deviation from ISMS requirements, potentially causing a system failure?

Option A : Observation

Option B : Minor Nonconformity

Option C : Major Nonconformity

Option D : Opportunity for Improvement

Correct Answer: C

Explanation/Reference:

A Major Nonconformity represents a severe breakdown in the ISMS, indicating a critical failure that could result in system failure or a significant security breach. This requires immediate corrective action and verification.

QUESTION: 11

Envision your organization plans to implement an ISMS. You are assigned the role of an internal auditor prior to the external certification audit. Which of the following actions is MOST aligned with the 'due professional care' principle during your internal audit?

- Option A : Accepting the initial scope definition without question to avoid disrupting the implementation process.
- Option B : Providing constructive feedback on identified nonconformities, even if it means potentially delaying the certification timeline.
- Option C : Focusing solely on easily verifiable controls to ensure a high rate of compliance and a positive audit result.
- Option D : Relying heavily on the expertise of the ISMS implementation team to streamline the audit process and minimize disruption.

Correct Answer: B

Explanation/Reference:

The principle of 'due professional care' requires auditors to exercise diligence, competence, and objectivity. While a smooth certification timeline is desirable, the auditor's primary responsibility is to provide accurate and constructive feedback to ensure the ISMS is robust and effective. Option 2 best reflects this commitment to thoroughness and objective assessment, even if it introduces potential challenges.

QUESTION: 12

Suppose a company 'SecureTech' holds ISO/IEC 27001 certification. During a surveillance audit, the auditor discovers several minor nonconformities relating to asset management. SecureTech promptly corrects these nonconformities and provides evidence to the auditor. What is the MOST appropriate auditor's response regarding the nonconformities?

- Option A : Recommend immediate suspension of SecureTech's ISO/IEC 27001 certification due to the observed nonconformities.
- Option B : Record the corrections as positive findings and disregard the initial nonconformities entirely.
- Option C : Accept the corrective actions as evidence of commitment to ISMS maintenance and allow the certification to continue without further action.
- Option D : Accept the corrective actions and record the nonconformities as closed, while potentially increasing the scope or frequency of future audits based on the number and nature of the findings.

Correct Answer: D

Explanation/Reference:

The auditor's role is to assess the ongoing effectiveness of the ISMS. While prompt correction of nonconformities is positive, ignoring the initial breach is inappropriate. Suspension is too drastic for minor issues. Option 4 offers the most appropriate response by acknowledging the issues, recording them for future reference, and adjusting the audit strategy if necessary to ensure continued improvement and compliance.

QUESTION: 13

Regarding the effectiveness of corrective actions after an ISO 27001 audit, what's the auditor's MOST important responsibility?

- Option A : Ensuring all corrective actions are implemented precisely as recommended by the auditor.
- Option B : Verifying that corrective actions address the root cause of the nonconformity and prevent recurrence.
- Option C : Approving the budget for implementing all corrective actions.
- Option D : Training the auditee's employees on the correct way to implement corrective actions.

Correct Answer: B

Explanation/Reference:

The auditor's most important responsibility is to verify that the corrective actions address the root cause of the nonconformity and prevent recurrence. This ensures the ISMS is improved effectively. While auditors can recommend corrective actions, it's ultimately the auditee's responsibility to implement them and management's responsibility to provide the necessary resources. Approving a budget or providing training are not core responsibilities of an ISMS auditor during the follow-up of corrective actions.

QUESTION: 14

In establishing an ISMS, which principle most directly addresses the ongoing monitoring and adjustment of security controls based on performance and changing threat landscape?

- Option A : Continual Improvement
- Option B : Risk-Based Thinking
- Option C : Management Responsibility
- Option D : Process Approach

Correct Answer: A

Explanation/Reference:

Continual Improvement, a core principle of ISO/IEC 27001, directly addresses the ongoing monitoring and adjustment of security controls. It involves systematically identifying opportunities for improvement, implementing changes, and evaluating their effectiveness. While Risk-Based Thinking informs the initial selection and prioritization of controls,

and Management Responsibility provides the framework for the ISMS, and Process Approach defines interactions, it is Continual Improvement that focuses on the dynamic nature of security management and the need for constant adaptation to maintain effectiveness against evolving threats.

THANK YOU FOR DOWNLOADING ISO-CLA-22 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our ISO-CLA-22 Exam Product

Visit Our Site to Purchase the Full Set of Actual ISO-CLA-22 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/gaqm/iso-cla-22-pdf-exam-dumps>