Free Questions for ISO-IEC-27001-Lead-Auditor by dumpshq

Shared by Cole on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which two of the following statements are true?

Options:

A- The role of a certification body auditor involves evaluating the organisation's processes for ensuring compliance with their legal requirements

B- Curing a third-party audit, the auditor evaluates how the organisation ensures that 4 6 made aware of changes to the legal requirements

C- As part of a certification body audit the auditor is resporable for verifying the organisation's legal compliance status

Answer:

A, B

Explanation:

The following statements are true:

The role of a certification body auditor involves evaluating the organization's processes for ensuring compliance with their legal requirements. This is part of the auditor's responsibility to assess the effectiveness and conformity of the organization's ISMS against the ISO/IEC 27001:2022 standard and the applicable legal and regulatory requirements.

During a third-party audit, the auditor evaluates how the organization ensures that they are made aware of changes to the legal requirements. This is part of the auditor's responsibility to verify that the organization has established and maintained a process for identifying and updating their legal and other requirements related to information security. The following statement is false:

As part of a certification body audit, the auditor is responsible for verifying the organization's legal compliance status. This is not true, as the auditor is not authorized or qualified to provide legal advice or judgment on the organization's compliance status. The auditor can only report on the evidence of compliance or noncompliance observed during the audit, but the ultimate responsibility for ensuring legal compliance lies with the organization.Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 66. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 67. :ISO/IEC 27001 LEAD AUDITOR - PECB, page 22.

Question 2

Question Type: MultipleChoice

Which one of the following options best describes the main purpose of a Stage 1 third-party audit?

Options:

A- To introduce the audit team to the client

B- To learn about the organisation's procurement

C- To determine redness for a stage 2 audit

D- To check for legal compliance by the organisation

E- To prepare an independent audit report

F- To get to know the organisation's customers

Answer:

C

Explanation:

The main purpose of a Stage 1 third-party audit is to determine readiness for a Stage 2 audit. A Stage 1 audit is a preliminary assessment that evaluates the organization's ISMS documentation, scope, context, and objectives, and identifies any major gaps or nonconformities that need to be addressed before the Stage 2 audit. A Stage 1 audit does not introduce the audit team to the client, as this is done during the audit planning phase. A Stage 1 audit does not check for legal compliance by the organization, as this is done during the Stage 2 audit. A Stage 1 audit does not prepare an independent audit report, as this is done after the Stage 2 audit.Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 70. :ISO/IEC 27001 LEAD AUDITOR - PECB, page 23.

Question 3

Question Type: MultipleChoice

A property of Information that has the ability to prove occurrence of a claimed event.

Options:

A- Electronic chain letters

B- Integrity

C- Availability

D- Accessibility

Answer:

B

Explanation:

A property of information that has the ability to prove occurrence of a claimed event is integrity. Integrity is one of the three main objectives of information security, along with confidentiality and availability. Integrity ensures that information and systems are not corrupted, modified, or deleted by unauthorized actions or events. Integrity also implies that information and systems can be verified and validated as authentic and accurate. Electronic chain letters are not a property of information, but a type of spam or hoax message that may contain malicious or misleading content. Availability means that service should be accessible at the required time and usable only by the authorized entity. Accessibility is not a property of information, but a characteristic of usability that refers to how easy it is for users to access and interact with information and systems.Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 13.

Question 4

Question Type: MultipleChoice

Information or data that are classified as ______ do not requirelabeling.

Options:

A- Public

B- Internal

C- Confidential

D- Highly Confidential

Answer:

A

Explanation:

Information or data that are classified as public do not require labeling. Public information or data are those that are intended for general disclosure and have no impact on the organization's operations or reputation if disclosed. Labeling is a method of implementing classification, which is a process of structuring information according to its sensitivity and value for the organization. Labeling helps to identify the level of protection and handling required for each type of information. Information or data that are classified as internal, confidential, or highly confidential require labeling, as they contain information that is not suitable for public disclosure and may cause harm or loss to the organization if disclosed.Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 34. : CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 37. : [ISO/IEC 27001 LEAD AUDITOR - PECB], page 14.

Question 5

Question Type: MultipleChoice

What is the standard definition of ISMS?

Options:

A- Is an information security systematic approach to achieve business objectives for implementation, establishing, reviewing,operating and maintaining organization's reputation.

B- A company wide business objectives to achieve information security awareness for establishing, implementing, operating, monitoring, reviewing, maintaining and improving

C- A project-based approach to achieve business objectives for establishing, implementing,operating, monitoring, reviewing, maintaining and improving an organization's information security

D- A systematic approach for establishing, implementing, operating,monitoring, reviewing, maintainingand improving an organization's information security to achieve business objectives.

Answer:

D

Explanation:

The standard definition of ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. This definition is given in clause 3.17 of ISO/IEC 27001:2022, and it describes the main components and purpose of an ISMS. An ISMS is not a project-based approach, as it is an ongoing process that requires continual improvement. An ISMS is not a company wide business objective, as it is a management system that supports the organization's objectives. An ISMS is not an information security systematic approach, as it is a broader concept that encompasses the organization's context, risks, controls, and performance.Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 15. : ISO/IEC 27001:2022, clause 3.17.

Question 6

Question Type: **MultipleChoice**

In the event of an Information security incident, system users' roles and responsibilities are to be observed, except:

Options:

A- Report suspected or known incidents upon discovery through the Servicedesk

B- Preserve evidence if necessary

C- Cooperate with investigative personnel during investigation if needed

D- Make the information security incident details known to all employees

Answer:

D

Explanation:

The role and responsibility that system users should not observe in the event of an information security incident is D: make the information security incident details known to all employees. This is not a proper role or responsibility for system users, as it could cause unnecessary panic, confusion or speculation among employees who are not involved in the incident response process. It could also compromise the confidentiality and integrity of the incident information, which could be sensitive or confidential in nature. Making the information security incident details known to all employees could also violate the information security policies and procedures of the organization, which may require a certain level of discretion and confidentiality when dealing with incidents. The other roles and responsibilities are correct, as they describe what system users should do in the event of an information security incident, such as reporting the incident to the Servicedesk (A), preserving evidence if necessary (B), and cooperating with investigative personnel if needed . These roles and responsibilities help to ensure a quick, effective and orderly response to information security incidents. ISO/IEC 27001:2022 requires the organization to implement procedures for reporting and managing information security incidents (see clause A.16.1).Reference:CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course,ISO/IEC 27001:2022 Information technology --- Security techniques --- Information security management systems --- Requirements,What is Information Security Incident Management?

Question 7

Question Type: MultipleChoice

The following are definitions of Information, except:

Options:

A- accurate and timely data

B- specific and organized data for a purpose

C- mature and measurable data

D- can lead to understanding and decrease in uncertainty

Answer:

C

Explanation:

The definition of information that is not correct is C: mature and measurable data. This is not a valid definition of information, as information does not have to be mature or measurable to be considered as such. Information can be any data that has meaning or value for someone or something in a certain context. Information can be subjective, qualitative, incomplete or uncertain, depending on how it is interpreted or used. Mature and measurable data are characteristics that may apply to some types of information, but not all. The other definitions of information are correct, as they describe different aspects of information, such as accuracy and timeliness (A), specificity and organization (B), and understanding and uncertainty reduction (D). ISO/IEC 27001:2022 defines information as "any data that has meaning" (see clause 3.25).Reference:CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course,ISO/IEC 27001:2022 Information technology --- Security techniques --- Information security management systems --- Requirements,What is Information?

20%
DISCOUNT