



Vendor: PECB

Exam Code: Lead-Auditor

Exam Name: PECB Certified ISO/IEC 27001 Lead Auditor

Version: DEMO

QUESTION 1

What is the difference between a restricted and confidential document?

- A. Restricted - to be shared among an authorized group
Confidential - to be shared among named individuals
- B. Restricted - to be shared among named individuals
Confidential - to be shared among an authorized group
- C. Restricted - to be shared among named individuals
Confidential - to be shared across the organization only
- D. Restricted - to be shared among named individuals
Confidential - to be shared with friends and family

Answer: B

Explanation:

The difference between a restricted and confidential document is that a restricted document is to be shared among named individuals, while a confidential document is to be shared among an authorized group. Restricted and confidential are examples of information classification levels that indicate the sensitivity and value of information and the degree of protection required for it. Restricted documents contain information that could cause serious damage or harm to the organization or its stakeholders if disclosed to unauthorized persons. Therefore, they should only be accessed by specific individuals who have a legitimate need to know and are authorized by the information owner. Confidential documents contain information that could cause damage or harm to the organization or its stakeholders if disclosed to unauthorized persons. Therefore, they should only be accessed by a defined group of people who have a legitimate need to know and are authorized by the information owner. ISO/IEC 27001:2022 requires the organization to classify information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification (see clause A.8.2.1).

QUESTION 2

CEO sends a mail giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it. The mail should be classified as

- A. Internal Mail
- B. Public Mail
- C. Confidential Mail
- D. Restricted Mail

Answer: A

Explanation:

The mail sent by the CEO giving his views on the status of the company and the company's future strategy and the CEO's vision and the employee's part in it should be classified as internal mail. Internal mail is a type of classification that indicates that the information is intended for internal use only, and should not be disclosed to external parties without authorization. The mail sent by the CEO contains information that is relevant and important for the employees of the company, but may not be suitable for public disclosure, as it may contain sensitive or confidential information about the company's performance, goals, or plans.

QUESTION 3

You see a blue color sticker on certain physical assets.
What does this signify?

- A. The asset is very high critical and its failure affects the entire organization

- B. The asset with blue stickers should be kept air conditioned at all times
- C. The asset is high critical and its failure will affect a group/s/project's work in the organization
- D. The asset is critical and the impact is restricted to an employee only

Answer: C

Explanation:

You see a blue color sticker on certain physical assets. This signifies that the asset is high critical and its failure will affect a group/s/project's work in the organization. A blue color sticker is a type of label that indicates the level of criticality of an asset, which is a measure of how important an asset is for the organization's operations and objectives. A high critical asset is an asset that has a significant impact on the organization's activities, and its loss or damage would cause major disruption or loss of service. A blue color sticker also implies that the asset requires a high level of protection and security, and should be handled with care.

QUESTION 4

Integrity of data means

- A. Accuracy and completeness of the data
- B. Data should be viewable at all times
- C. Data should be accessed by only the right people

Answer: A

Explanation:

Integrity of data means accuracy and completeness of the data. 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. Data should be viewable at all times is not related to integrity, but to availability. Data should be accessed by only the right people is not related to integrity, but to confidentiality.

QUESTION 5

You have a hard copy of a customer design document that you want to dispose off. What would you do

- A. Throw it in any dustbin
- B. Shred it using a shredder
- C. Give it to the office boy to reuse it for other purposes
- D. Be environment friendly and reuse it for writing

Answer: B

Explanation:

The best way to dispose of a hard copy of a customer design document is to shred it using a shredder. This is because shredding ensures that the document is destroyed and cannot be reconstructed or accessed by unauthorized persons. A customer design document may contain sensitive or confidential information that could cause harm or damage to the customer or the organization if disclosed. Therefore, it is important to protect the confidentiality and integrity of the document until it is securely disposed of. Throwing it in any dustbin, giving it to the office boy to reuse it for other purposes, or reusing it for writing are not secure ways of disposing of the document, as they could expose the document to unauthorized access, theft, loss or damage. ISO/IEC 27001:2022 requires the organization to implement procedures for the secure disposal of media containing information (see clause A.8.3.2).

QUESTION 6

You receive the following mail from the IT support team: Dear User, Starting next week, we will be deleting all inactive email accounts in order to create space. Share the below details in order to continue using your account. In case of no response,

Name:

Email ID:

Password:

DOB:

Kindly contact the webmail team for any further support. Thanks for your attention.

Which of the following is the best response?

- A. Ignore the email
- B. Respond it by saying that one should not share the password with anyone
- C. One should not respond to these mails and report such email to your supervisor

Answer: C

Explanation:

The best response to the email from the IT support team asking for personal details is to not respond to the email and report it to your supervisor. The email is likely a phishing attempt, which is a form of social engineering that uses deceptive emails or other messages to trick recipients into revealing sensitive information, such as passwords, credit card numbers, bank account details, etc. Phishing emails often impersonate legitimate organizations or individuals and create a sense of urgency or curiosity to lure the victims into clicking on malicious links, opening malicious attachments or providing personal information. The IT support team should never ask for your password or other personal details via email, as this is a violation of information security policies and best practices. Ignoring the email or responding to it by saying that one should not share the password with anyone are not sufficient responses, as they do not alert the IT support team or your supervisor about the phishing attempt, which could affect other users as well. Reporting the email to your supervisor is a responsible action that could help prevent further damage or compromise of information. ISO/IEC 27001:2022 requires the organization to implement awareness and training programs to make users aware of the risks of social engineering attacks, such as phishing, and how to avoid them (see clause A.7.2.2).

QUESTION 7

The following are definitions of Information, except:

- 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.

QUESTION 8

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

observed, except:

- 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.

QUESTION 9

What is the standard definition of ISMS?

- 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, maintaining and 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.

QUESTION 10

All are prohibited in acceptable use of information assets, except:

- A. Electronic chain letters
- B. E-mail copies to non-essential readers
- C. Company-wide e-mails with supervisor/TL permission.
- D. Messages with very large attachments or to a large number of recipients.

Answer: C

Explanation:

The only option that is not prohibited in acceptable use of information assets is C: company-wide e-mails with supervisor/TL permission. This option implies that the sender has obtained the necessary authorization from their supervisor or team leader to send an e-mail to all employees in the organization. This could be done for legitimate business purposes, such as announcing important news, events or updates that are relevant to everyone. However, this option should still be used sparingly and responsibly, as it could cause unnecessary disruption or annoyance to the recipients if abused or misused.

QUESTION 11

In acceptable use of Information Assets, which is the best practice?

- A. Access to information and communication systems are provided for business purpose only
- B. Interfering with or denying service to any user other than the employee's host
- C. Playing any computer games during office hours
- D. Accessing phone or network transmissions, including wireless or wifi transmissions

Answer: A

Explanation:

The best practice in acceptable use of information assets is A: access to information and communication systems are provided for business purpose only. This means that the organization grants access to its information and communication systems only to authorized users who need to use them for legitimate and approved business activities. The organization does not allow or tolerate any unauthorized, inappropriate or personal use of its information and communication systems, as this could compromise information security, violate policies or laws, or cause damage or harm to the organization or its stakeholders.

QUESTION 12

CMM stands for?

- A. Capability Maturity Matrix
- B. Capacity Maturity Matrix
- C. Capability Maturity Model
- D. Capable Mature Model

Answer: C

Explanation:

Capability Maturity Model (CMM) is a framework that describes the key elements of an effective software process. It defines five levels of maturity for software development organizations, from initial to optimized. The CMM helps organizations to assess their current level of process capability and identify the areas for improvement.

QUESTION 13

Which is not a requirement of HR prior to hiring?

- A. Undergo background verification
- B. Applicant must complete pre-employment documentation requirements
- C. Must undergo Awareness training on information security.
- D. Must successfully pass Background Investigation

Answer: C

Explanation:

According to ISO/IEC 27001:2022, clause 7.2.2, the organization shall ensure that all persons who have access to information are aware of the information security policy and their contribution to the effectiveness of the ISMS, including the benefits of improved information security performance. Therefore, awareness training on information security is a requirement for all persons, not just new hires.

QUESTION 14

Who are allowed to access highly confidential files?

- A. Employees with a business need-to-know
- B. Contractors with a business need-to-know
- C. Employees with signed NDA have a business need-to-know
- D. Non-employees designated with approved access and have signed NDA

Answer: A

Explanation:

According to ISO/IEC 27001:2022, clause 8.2.1, the organization shall ensure that access to information and information processing facilities is limited to authorized users based on the access control policy and in accordance with the business requirements of access control. Therefore, only employees with a business need-to-know are allowed to access highly confidential files, and not contractors, non-employees or employees with signed NDA.

QUESTION 15

Which is the glue that ties the triad together

- A. Process
- B. People
- C. Collaboration
- D. Technology

Answer: D

Explanation:

The triad refers to the three elements of information security: confidentiality, integrity and availability. Technology is the glue that ties the triad together, as it provides the means to implement various controls and measures to protect information from unauthorized access, modification or loss.

QUESTION 16

Implement plan on a test basis - this comes under which section of PDCA

- A. Plan
- B. Do
- C. Act
- D. Check

Answer: B

Explanation:

The PDCA cycle is a four-step method for managing and improving processes. The steps are Plan, Do, Check, and Act. In the Plan phase, the objectives and scope of the process are defined, and the resources and activities are planned. In the Do phase, the process is implemented on a test basis, and the results are recorded and analyzed.

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14