



**Free Questions for ISO-IEC-27001-Lead-Auditor by certscare**

**Shared by Barr on 24-05-2024**

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

---

## Question Type: MultipleChoice

---

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?

### Options:

---

**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).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 Phishing?

## Question 2

---

**Question Type:** MultipleChoice

---

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

### Options:

---

- 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).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 Secure Disposal?

## Question 3

---

**Question Type:** MultipleChoice

---

Integrity of data means

### Options:

---

- 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. Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 24. : [ISO/IEC 27001 Brochures | PECB], page 4.

## **Question 4**

---

**Question Type:** MultipleChoice

---

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

### **Options:**

---

**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. Reference:: CQI & IRCA ISO 27001:2022 Lead Auditor Course Handbook, page 36. : [ISO/IEC 27001 Brochures | PECB], page 6.

## Question 5

---

**Question Type:** MultipleChoice

---

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

**Options:**

---

- 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. 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 6

---

**Question Type:** MultipleChoice

---

What is the difference between a restricted and confidential document?

### Options:

---

**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).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 Classification?

**To Get Premium Files for ISO-IEC-27001-Lead-Auditor Visit**

**<https://www.p2pexams.com/products/iso-iec-27001-lead-auditor>**

**For More Free Questions Visit**

**<https://www.p2pexams.com/pcb/pdf/iso-iec-27001-lead-auditor>**

