IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

Exam : **ISO-IEC-27001 Lead Auditor**

Title : PECB Certified ISO/IEC 27001 Lead Auditor exam

Version : DEMO

1.Changes on project-managed applications or database should undergo the change control process as documented.
A. True
B. False
Answer: A
Explanation:
Changes on project-managed applications or database should undergo the change control process as documented, because this is a requirement of ISO/IEC 27001:2022 clause 12.1.2, which states that “the organization shall define and apply a change management process for changes to systems and applications within the scope of the information security management system”. The change management process should ensure that changes are recorded, assessed, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.
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]

2.A scenario wherein the city or location where the building(s) reside is / are not accessible.
A. Component
B. Facility
C. City
D. Country
Answer: C
Explanation:
A scenario wherein the city or location where the building(s) reside is / are not accessible is called a city disaster scenario, according to the CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course. This scenario is one of the four types of disaster scenarios that should be considered in the business continuity planning process, along with component, facility and country scenarios. A city scenario may be caused by events such as natural disasters, civil unrest, terrorist attacks or pandemic outbreaks that affect the entire city or region where the organization operates.
Reference: [CQI & IRCA Certified ISO/IEC 27001:2022 Lead Auditor Training Course]

3.What would be the reference for you to know who should have access to data/document?
A. Data Classification Label
B. Access Control List (ACL)
C. Masterlist of Project Records (MLPR)
D. Information Rights Management (IRM)
Answer: B
Explanation:
The reference for you to know who should have access to data/document is the Access Control List (ACL), which is a list of users or groups who are authorized to access a specific data/document and their respective access rights (such as read, write, modify, delete, etc.). The ACL is a tool for implementing the access control policy of the organization, which is defined in accordance with ISO/IEC 27001:2022 clause 9.4.1. The ACL should be maintained and updated regularly to ensure that only authorized users can access the data/document.

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]

4.An employee caught with offense of abusing the internet, such as P2P file sharing or video/audio streaming, will not receive a warning for committing such act but will directly receive an IR.
A. True
B. False
Answer: A
Explanation:
An employee caught with offense of abusing the internet, such as P2P file sharing or video/audio streaming, will not receive a warning for committing such act but will directly receive an IR, because this is a violation of the organization's information security policy and acceptable use policy. An IR (incident report) is a formal document that records the details of an information security incident and the actions taken to resolve it. An IR may also trigger disciplinary actions against the employee, depending on the severity and impact of the incident.
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], Example of an information security policy, Example of an acceptable use policy

5.An employee caught temporarily storing an MP3 file in his workstation will not receive an IR.
A. True
B. False
Answer: B
Explanation:
An employee caught temporarily storing an MP3 file in his workstation will receive an IR, because this is also a violation of the organization's information security policy and acceptable use policy. An MP3 file is a type of media file that may contain copyrighted or illegal content, or may introduce malware or viruses into the organization's network. The employee should not store any unauthorized or personal files in his workstation, as this may compromise the confidentiality, integrity and availability of the organization's information assets.
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], Example of an information security policy, Example of an acceptable use policy