



**Exam Name – ISO 28000 - Certified Lead Auditor**

**Exam Code – ISO-28000-CLA**

**Sample Exam**

The standard ISO 28000 specifies the requirement for:

- A) Security management system for supply chain
- B) Information security management system
- C) Business continuity management system
- D) Safety management systems

Answer: A

PDCA Refers to

- A. Plan Do Correct Acknowledge
- B. Plan Define Check Act
- C. Plan Do Check Act
- D. Please Do and Check Accordingly

Answer: C



As per the ISO 28000 standard internal audit shall be conducted?

- A. Always Every Year
- B. At planned Intervals
- C. Prior to Certification audit
- D. As per management availability

Answer: B

According to ISO 28000, security risk assessment shall consider risks due to:

- A. Physical failure threats and risks
- B. Operational threats and risks
- C. Stakeholder threats and risks
- D. All of the above

Answer: D



To address the root cause(s) of a nonconformity the company will implement

- A. One or several corrective actions
- B. One or several corrections
- C. Corrective actions and preventive actions
- D. None of the above

Answer: A

According to ISO 28000, Security management objectives shall be

- A. Consistent with commitment to supplier evaluation ratings
- B. One-time activity
- C. Communicated to Regulatory body
- D. Communicated, documented and reviewed periodically
- E. Approved by Regulatory body

Answer: D



In accordance with ISO 28000, which of the following requires records to be retained by the organization?

- A. Training and competence records
- B. Security inspection reports
- C. Reports of security exercises and drills
- D. All of the above

Answer: D