ISO 27001 Lead Auditor

1. **During an audit interview, the Chief Information Security Officer (CISO) discussed the risk of a loss of availability of the web application services. It was noted that the security information risk process had identified that the owner of risks associated with the loss of availability would be the Customer Services Manager.**
   Which should the auditor expect to be documented in order to confirm that this risk is being treated appropriately?

A. Actions to be taken by the CISO to achieve continual improvement.

B. The Customer Services Manager was responsible for risk treatment.

C. Acceptance of the residual risk by the Customer Services Manager.

D. Criteria for performing information security risk assessments.

2. **Recently, an existing customer has gained ISO 27001 certification and they have written to the Sales Director setting out the information they will now require. This information will enable the audit of their suppliers and will need to appear in future contracts with all their suppliers. Which topic-specific policy within the policies for information security control should the auditor review in order to assess whether these new requirements have been dealt with appropriately?**

A. Information classification.

B. Supplier relationships.

C. Mobile devices and teleworking.

D. Information transfer.

3. **When preparing the audit conclusions, how should an auditor make a suggestion to improve the efficiency of a process?**

A. By giving a recommendation of a suitable tool for improving the process.

B. By offering to help the auditee find a better tool to undertake the task.

C. By instructing the auditee to change their existing process to a better process.

D. By noting a nonconformity against a specific control or controls.

4. **What is meant by the audit principle of 'fair presentation' according to ISO 19011?**

A. Auditors should exercise restraint in their personal views when auditing.

B. Auditors should report accurately any differences in views.

C. Auditors should carry out their work with discretion and responsibility.

D. Auditors should carry out their work according to procedures.

5. **An audit is being carried out in an organization with a mature information security management system. The helpdesk logs showed a very high occurrence of password resetting requests from users. What evidence should the auditor expect to see in the password policy to ensure that the requirements of the password management system control are being met?**

A. Explains how passwords can be reset remotely by the users.

B. States that the system will allow the same password to be used.

C. Explains that certain systems that contain sensitive information require a second login.

D. States that the initial passwords must be changed after seven days.

6. **Which of the following are carried out by a certification body during stage 2 of a certification audit?**

1. Observing daily activities dealing with information security risk

2. Reviewing the documented procedures for risk assessment

3. Interviewing customer staff affected by information security risks

4. Assessing the information security risk process operational logs

A. 1, 2, 3

B. 1, 2, 4

C. 2, 3, 4

D. 1, 3, 4

7. **During an interview, the auditor found out that a human resources employee was rather overzealously removing access rights for contractors on the last day of their contract, even though the contractors had been extended on their projects. It appeared that the process to notify HR of any extensions was not working smoothly and effort was wasted reinstating access.**
   Is it appropriate for the auditor to categorise the control for termination or change of employment responsibilities as an observation?

A. No, because this control is lacking in enforcement and should be categorised as a minor nonconformity.

B. Yes, because the control is being enforced, but there is an opportunity for improvement.

C. Yes, because human resources procedures would be out of scope of the ISMS.

D. No, because the contractor's access rights had been incorrectly rescinded.

8. **A director has had their laptop bag stolen. Although the laptop was encrypted, the director's bag also contained paper documents describing sensitive commercial details. Which action would satisfy the auditor that the procedures for the 'collection of evidence' within the information security incident management control had been applied appropriately?**

A. Travelling directors were immediately provided with encrypted tablet PCs to use in place of paper documents.

B. The Chief Information Officer assigned an Information Security Officer to formally investigate the episode.

C. The director immediately informed the local police of the theft.

D. The director received a Police Report after reporting the event to the police.

9. **During an audit interview with the Facilities Manager, it was noted that the Facilities department had reorganized the responsibilities of staff after many entrance swipe cards had not been returned. The responsibility for monitoring who held entrance swipe cards and ensuring cards are returned had been moved from the building security officers to a single junior role on the Facilities Help Desk who was trained in the entrance security system.**
What should the auditor review in order to assess the competence of staff in relation to this reorganization?

A. Timesheets completed by the junior level staff member with swipe card responsibilities.

B. Evidence held by the department that fewer swipe cards are going missing after reorganization.

C. Staff morale of the building security officers at losing the swipe card responsibilities.

D. Staff morale of the building security officers at losing the swipe card responsibilities.

10. **Which outcome from an audit can be graded into minor and major?**

A. Nonconformity

B. Conformity

C. Outside the audit scope

D. Observation

11. **Which situation describes appropriate evidence collected by an auditor?**

A. Verbal statements from a Chief Operations Officer are always considered to be reliable evidence.

B. A verbal statement is reliable if corroborated by an implementation of change.

C. The best evidence that can be gathered will be acceptable even if unverified.

D. The auditor can use their judgment if there is poor verification of a verbal statement