Procom is a mid-sized manufacturer of electronic goods with headquarters in Pakistan and factories located in Afghanistan. An IS auditor within the enterprise has been asked to perform preliminary work that will assess the organization’s readiness for a review to measure compliance with new Pakistani regulatory requirements.

These requirements are designed to ensure that management is taking an active role in setting up and maintaining a well-controlled environment and will assess management’s review and testing of the general IT controls. Areas to be assessed include:

• Logical and physical security

• Change management

• Production control and network management

• IT governance

• End-user computing

The IS auditor has been given six months to perform this preliminary work. In previous years, repeated problems have been identified in the areas of logical security and change management. Logical security deficiencies noted included the sharing of administrator accounts and failure to enforce adequate controls over passwords. Change management deficiencies included improper segregation of incompatible duties and failure to document all changes. Additionally, the process for deploying operating system updates to servers was found to be only partially effective. In anticipation of the work to be performed by the IS auditor, the chief information officer (CIO) requested direct reports to develop narratives and process flows describing the major activities for which IT is responsible.

These were completed, approved by the various process owners and the CIO, and then forwarded to the IS auditor for examination.

**1. What should the IS auditor do FIRST?**

1. Perform a survey audit of logical access controls.
2. Revise the audit plan to focus on risk-based auditing.
3. Perform an IT risk assessment.
4. Begin testing controls that the IS auditor feels are most critical.

**2. When auditing the logical security, the IS auditor is MOST concerned when observing:**

1. The system administrator account is known by everybody.
2. The passwords are not enforced to change frequently.
3. The network administrator is given excessive permissions.
4. The IT department does not have written policy on privilege

**3. When testing program change management in this case, how should the sample be selected?**

1. Change management documents should be selected at random and examined for appropriateness.
2. Changes to production code should be sampled and traced to appropriate authorizing documentation.
3. Change management documents should be selected based on system criticality and examined for appropriateness.
4. Changes to production code should be sampled and traced back to system-produced logs indicating the date and time of the change.

After the preliminary work has been completed, Procom decides to plan audits for the next two years. After accepting the appointment, the IS auditor notes that:

* The entity has an audit charter that details the scope and responsibilities of the IS audit function and specifies the audit committee as the overseeing body for audit activity.
* The entity is subject to regulatory compliance requirements that require its management to certify the effectiveness of the internal control system as it relates to financial reporting.
* The entity has been recording consistent growth over the last two years at double the industry average.
* The entity has seen increased employee turnover as well.

**4. The FIRST priority of the IS auditor in year one should be to study the:**

1. Previous IS audit reports and plan the audit schedule.
2. Audit charter and plan the audit schedule.
3. Impact of the increased employee turnover.
4. Impact of the implementation of a new ERP on the IT environment.

**5. How should the IS auditor evaluate backup and batch processing within computer operations?**

1. Rely on the service auditor’s report of the service provider.
2. Study the contract between the entity and the service provider.
3. Compare the service delivery report to the service level agreement.
4. Plan and carry out an independent review of computer operations.

**6. During the day-to-day work, the IS auditor advises there is a risk that log review may not result in timely detection of errors. This is an example of which of the following:**

1. inherent risk
2. residual risk
3. control risk
4. material risk
5. **In performing a risk-based audit, which risk assessment is completed FIRST by an IS auditor?**
6. Detection risk assessment
7. Control risk assessment
8. Inherent risk assessment
9. Fraud risk assessment
10. **Which of the following types of audit risk assumes an absence of compensating controls in the area being reviewed?**
11. Control risk
12. Detection risk
13. Inherent risk
14. Sampling risk
15. **An IS auditor performing a review of an application’s controls finds a weakness in system software that could materially impact the application. In this situation, an IS auditor should:**
16. Disregard these control weaknesses because a system software review is beyond the scope of this review.
17. Conduct a detailed system software review and report the control weaknesses.
18. Include in the report a statement that the audit was limited to a review of the application’s controls.
19. Review the system software controls as relevant and recommend a detailed system software review.
20. **Which of the following would an IS auditor perform FIRST when planning an IS audit?**
21. Define audit deliverables.
22. Finalize the audit scope and audit objectives.
23. Gain an understanding of the business’s objectives and purpose.
24. Develop the audit approach or audit strategy.