ISO 27001 Internal Auditor (I27001IA)

Supporting Questions V112023

1. In which of its clauses ISO 27001:2022 asks to consider:

a. Stakeholders that are relevant to the information security management system
b. The requirements of these stakeholders that are relevant to information security.
c. Which of these requirements will be addressed through the Information Security Management System.

2. ISO 27001:2022 states that when the organization determines the need for changes to the ISMS, the changes shall be carried out in a planned manner in its clause:

a) Clause 6.3
b) Clause 10.2
c) Clause 4.2

3. Annex A of ISO 27001:2022 defines 4 categories (organizational, people, physical and technological) to group the 93 information security controls.

a) True
b) False

4. Once the audit has been carried out, the auditor in charge of the audit must prepare the Audit Report. This report establishes:

    a. Audit objectives
    b. Scope of the audit.
    c. Auditees and the audit period.
    d. Documentation of the contact person.
    e. Documentation of the lead auditor and other auditors.
    f. Dates and locations where the audit activities took place.
    g. Audit criteria.
    h. Audit statements.
    i. Audit Conclusions.

a) All are correct.
b) All except d and e.
c) Only i.

5. The audit objectives define what is to be achieved with the individual audit.

a) True.
b) False.

6. The Statement of Applicability (SoA) must contain:

    a. The controls necessary to implement the chosen information security risk treatment option(s).
    b. Justification of inclusions.
    c. Whether or not the necessary controls are implemented.
    d. Justification for exclusions from any of the controls in annex A.

a) All are correct.
b) All except b and c.
c) Only a.

7. During the closing meeting the lead auditor should explain, for example, any related post-audit activities (e.g., implementation and review of corrective actions, handling of audit complaints, appeals process).

a) True.
b) False.

8. Regarding documented information, ISO 27001:2022 indicates it may include:

a) Documented information of external origin, determined by the organization as necessary for the planning and operation of the information security management system.
b) Documented information required by the information security management system and by this international regulation.
c) Documented information that the organization has determined is necessary for the effectiveness of the information security management system.
d) All of the above.

9. The audit plan refers to:

a) A set of one or more audits planned for a specific period of time and directed toward a specific purpose.
b) Description of the activities and arrangements for an audit.

10. ISO 19011:2018 determines nonconformities and improvement opportunities as noncompliance to requirements of the audited regulation.

c) True.
d) False.

11. This is the best time to disclose the conditions under which the audit may be terminated.

a) At the beginning of an individual audit.
b) At the opening meeting.
c) During the definition of the audit scope.

12. ISO 17011:2018 states that auditors should have knowledge and skills such as:

a) Understand the types of risks and opportunities associated with the audit.
b) Plan and organize work effectively.
c) Perform the audit within the agreed schedule.
d) Taking too much time to write their notes correctly.
e) Prioritize and focus on important issues.
f) Empower in the audit to try to obtain as much evidence as possible.
g) Communicate effectively, orally and in writing (either in person or through the use of interpreters).
h) Gather information through effective interviewing, listening, observing and reviewing documented information, including records and data.
i) All of the above are skills that an auditor should develop.
j) All except D and F.

13. During an interview it is best to ask leading questions (YES or NO questions), open-ended questions may confuse the auditee.

a) True.
b) False.

14. The questions: who?, how?, why?, why?, when?, where?, are:

a) Open-ended questions.
b) Closed-ended questions.

15. Checklists used by auditors:

a) Ensure that nothing important is overlooked.
b) Help provide information on any related post-audit activities (e.g., implementation and review of corrective actions, handling of audit complaints, appeal process).
c) Help to provide continuity to the audit.
d) Help provide information on possible consequences of not adequately addressing audit findings.
e) All of the above.
f) All except B and D.
g) B and D only.

16. They are responsible for designating the members of the audit team, including the team leader and any technical experts required for the specific audit.

a) The CISO.
b) The individual(s) managing the audit program.
c) The Lead Auditor.
d) The person in charge of the management.

17. It is a set of one or more audits planned for a specific period of time and directed towards a specific purpose.

a) Audit program.
b) Audit plan.
c) Checklists.
d) Audit scope.

18. These are types of audits:

a) Part one.
b) Part two.
c) Part three.
d) All of the above
e) Audits are only classified as internal or external.

19. Audit performed by or on behalf of the organization itself, i.e. with its own resources.

a) Part one.
b) Part two.
c) Part three.

20. Objective evidence:

a) Is data that supports the existence or truth of something.
b) Can be obtained through observation, measurement, testing or by other means.
c) It is an audit method to reach reliable conclusions.
d) All of the above
e) A and B only
f) A and C only

21. The results of the audit:

a) Are the evaluation results of the audit evidence gathered against the audit criteria.
b) They are considered findings and can be classified as conformity or nonconformity.
c) It is an audit method to reach reliable conclusions.
d) If the audit criteria are selected from legal requirements or regulatory requirements, the audit finding is referred to as compliance or noncompliance.
e) B and C only
f) A and C only
g) All of the above

22. It establishes that the organization must define a risk assessment process:

a) Clause 6.1.1
b) Clause 6.1.2
c) Clause 8.1
d) B and C are valid

23. It establishes that the organization must implement the risk treatment process:

a) Clause 6.1.2
b) Clause 6.1.3
c) Clause 8.3
d) B and C are valid

24. These are risk management strategies except:

a) Mitigate
b) Transfer
c) Assume
d) Retain
e) Control

25. Type of strategy where the implementation of a control to reduce the level of risk is defined:

a) Mitigate
b) Transfer
c) Assume
d) Retain

26. The "Statement of Applicability" must contain:

a) Controls necessary to reduce the level of risk.
b) The justification for the inclusion of the controls considered necessary.
c) Whether or not the necessary controls are implemented.
d) Justification for exclusions from any of the controls in annex A.
e) All are valid
f) B and D only

27. According to ISO 17011:2018 audit is defined as a systematic, independent, documented process for obtaining evidence and evaluating it objectively, in order to determine the extent to which the audit criteria are met.

a) True
b) False

28. ISO 19011:2018 establishes as methods for assessing auditors:

a) Observation
b) Examination
c) Interview
d) Telephone call
e) All are valid
f) All except D

29. During the audit, professional behavior by the auditor is desired, e.g., the auditor is expected to be open-minded, i.e., willing to consider alternative ideas or points of view.

a) True
b) False

30. Defining objectives, scope and criteria for each individual audit, Selecting audit methods, and Defining and implementing the necessary operational controls for the supervision of the audit program are part of the activities for:

a) Define the scope of the ISMS.
b) Correctly create the ISMS policy.
c) Define the audit program.

31. They are responsible for assigning responsibilities to the audit team:

a) The Lead Auditor.
b) The person responsible for the management system.
c) Senior management.
d) The person(s) managing the audit program.

32. They should ensure that the following activities are carried out as part of the management of the results of the audit program:

1. Evaluation of the achievement of the objectives for each audit within the audit program.
2. Review and approval of audit reports on compliance with the scope and objectives of the audit.
3. Reviewing the effectiveness of actions taken to address audit findings.
4. Distribution of audit reports to relevant stakeholders.
5. Determination of the need for any follow-up audits.

a) Members of the audit team.
b) Everyone in the organization.
c) The person(s) managing the audit program.

33. The audit plan describes:

a) The activities and arrangements for each planned audit.
b) A planning over a given period of time of one or more audits.
c) Both are valid since there is a relation between the program and the audit plan.

34. The audit program describes:

a) The activities and arrangements for each planned audit
b) A planning over a given period of time of one or more audits.
c) Both are valid since there is a relation between the program and the audit plan.

35. During an audit it is recommended to ask closed-ended questions, questions whose answer is YES or NO. This allows the audit to be more accurate.

a) True
b) False

36. During an audit the auditee provides little information and constantly rephrases the auditor's questions:

a) Considered difficult situations that the auditor must be able to handle.
b) Issues that the lead auditor must resolve.
c) Conditions for termination of the audit.

37. A finding indicates:

a) Conformity or nonconformity.
b) Compliance or noncompliance.
c) Both are valid.

38. An opportunity for improvement is not considered a nonconformity but may be reviewed by the organization, when deemed appropriate, to improve the effectiveness of the process.

a) True
b) False

39. They select and determine the methods for conducting the audit depending on the defined audit objectives, scope and criteria.

a) The audit team.
b) The lead auditor
c) Senior management
d) The person(s) managing the audit program.

40. The following are methods for performing audits.

1. On site.
2. Remote.
3. With human interaction
4. No human interaction.

a) Only 1 and 2
b) All except 4
c) Only 3 and 4
d) All

41. The audit team leader, in consultation with the audit team, assigns each team member responsibility for:

1. Auditing processes.
2. Activities.
3. Functions.
4. Developing the audit program.

a) Only 1 and 2
b) All except 4
c) Only 3 and 4
d) All

Answers

1. C
2. A
3. A
4. A
5. A
6. A
7. A
8. D
9. B
10. B
11. B
12. J
13. B
14. A
15. F
16. B
17. A
18. D
19. A
20. E
21. G
22. B
23. C
24. E
25. A
26. E
27. A
28. F
29. A
30. C
31. A
32. C
33. A
34. B
35. B
36. A
37. D
38. A
39. E
40. D
41. B