

IS Audit Process - Answer to Questions

1. *Answer: B*

The correct answer is B. How many controls are in place has little bearing on what the scope of the audit should be. Scope is a definition of what should be covered in the audit. What management is concerned about (A), what the management risk environment is (C), and how complex the technical environment is (D) could all have an impact of what the scope of a particular audit might be but not the sheer number of controls.

2. *Answer: C*

The correct answer is C. IS audit standards are mandatory to follow at all times unless justification exists for deviating from them. Complying with standards is one of the tenants of the IS Audit Code of Ethics and is not a guideline (A), does not apply only when the work needs to be defensible (B), or when regulatory or legal issues are involved (D).

3. *Answer: D*

The correct answer is D. When the perception of auditor independence is questioned, the audit management must investigate and determine whether the situation warrants actions such as removing the auditor or investigating further. There is no standard like the one mentioned, but the subject is covered in the organizational relationship and independence standard. The other answers are guidelines provided by ISACA.

4. *Answer: C*

The correct answer is C. Use of client information is unethical and a cause for revocation of your certification. The other three are tenants of the code of ethics.

5. *Answer: A*

The correct answer is A. Due care is a level of diligence applied to work performed. It is a reasonably competent third-party test. It does not ensure that no wrong conclusions are made (C) and is not related to a skill level (D) but a competence and prudence level. It is not a level of best effort (B). It is a benchmark to compare efforts against—that which would have been done in similar circumstances by a prudent and competent person.

6. *Answer: C*

The correct answer is C. You do not want to eliminate risk (A), you want to only manage and control it. Management's tolerance of the risk is part of the definition of what is material so whether the risk is material (B) is not a correct answer. Insurance coverage is not necessarily the only control to consider for mitigating residual risk (D). The correct balance of

cost to control any potential losses is a very important part of the risk mitigation considerations.

7. *Answer: D*

The correct answer is D. Answer A is the definition of an inherent risk, which is a risk in its natural state or without controls. A controls risk (B) is the chance that controls put in place will not solve the problem soon enough to prevent loss. A detection risk (C) occurs when auditing does not discover material errors due to sampling or testing procedures.

8. *Answer: A*

The correct answer is A. All of the items listed are relevant, however, by itself the maturity of the technology has the least amount of bearing on the risk assessment of an organization. Just because it is a mature technology does not mean it is inherently risky or does not meet the needs of the business.

9. *Answer: D*

The correct answer is D. While both are after the fact (A), the order of application is not really relevant. While corrective controls keep errors from resulting in loss (B), detective controls do not warn, deterrent controls do. While reasonableness checks can be a detective control, it also is used to make errors known (C).

10. *Answer: B*

The correct answer is B. The other three are pervasive because they focus on the management and monitoring of the overall IS infrastructure. Humidity controls are specific to a single data center only.

11. *Answer: D*

The correct answer is D. Independence from influence and for reporting purposes is the primary reason to have reporting lines outside of the corporate reporting structure.

12. *Answer: C*

The correct answer is C. The industry's best practices must be tempered by management tolerance for risk and their direction. The elimination of risks is not your goal. Risk is only relevant to management's needs.

13. *Answer: C*

The correct answer is C. Annual loss expectancy is the total losses both direct and indirect times the frequency of occurrence for that loss in a given year.

14. *Answer: A*

The correct answer is A. Materiality is a relative, professional judgment call that must take into context management's aggregate tolerance of risk, how this finding stacks up to all of the findings, and the potential cumulative effect of this error.

15. Answer: D

The correct answer is D. None of the above is *not* an auditing irregularity or a possible illegal act based on the definition in the standard.

16. Answer: A

The correct answer is A. While the others have varying relevance to audit testing, they do not indicate possible irregularities by themselves. A vacation policy that does not require staff to be away from work for a fixed period of time—usually one to two full weeks—enables employees to maintain fraudulent schemes without requiring a trained back up employee to step in and perform the process for at least some period of time during the year.

17. Answer: A

The correct answer is A. Some of the other answers are nonsensical, but the real reason for using the element of surprise is to ensure that the policies and procedures documents line up with actual practices.

18. Answer: C

The correct answer is C. The fact that this was their job at another company may actually be an advantage for the audit team. The other items listed could lead to a compromise of the auditor's independence and should be investigated.

19. Answer: A

The correct answer is A. The scope is not defined exclusively by the auditor (C) and does not necessarily define testing the related tasks (D). Answer B is somewhat correct; however, Answer A is the best answer.

20. Answer: D

The correct answer is D. The charter's main purpose is to define the auditor's roles and responsibilities. It should evidence a clear mandate and authority for the auditors to perform their work. Unlike a mission statement (B) or a process document (A), it describes the bounds of authority. The code of ethics (C) is a nonrelevant answer to this exercise.

21. Answer: B

The correct answer is B. Sampling satisfies the evidence requirements that the data is sufficient, reliable, relevant, useful, and supported by the

appropriate analysis. A random population section (D) is the definition of a random sample. Answers A and C do not make sense.

22.*Answer: C*

The correct answer is C. The rest of the answers list types of audit evidence that could be considered, but the auditor must consider the best evidence available and determine what method for gathering and reviewing it as a second step in the audit planning process.

23.*Answer: D*

The correct answer is D. There is no sampling error with CAATs, which is one of their strengths (A), you will need to be aware of other participants in the process but that should be under your control (B), and understanding whether the source and object code match is an issue with what you are testing not to itself (C). The best answer is that you should be concerned with the potential impact of your testing on live data.

24.*Answer: C*

The correct answer is C. Answer A is not value-added to the client; neither is D unless there is a weakness identified first. Answer B is an okay answer, however, Answer C is the best possible choice.

25.*Answer: B*

The correct answer is B. Materiality, audit objectives, and management's direction are the key items to consider. Answer D needs resolving long before the findings are reviewed for reportability; Answer A, how many, or Answer C, the effect of the recommendations, is not an issue with whether they should be reported or not.

26.*Answer: D*

The correct answer is D. Answers B and C are not correct because they are related to recommendations and not to the root cause. Answer A is a technique used in root cause analysis. The best answer is D.

27.*Answer: A*

The correct answer is A. The other answers are all important but the primary reason is one of ensuring due professional care by checking the work with a reasonably competent third-party review.