CISA Notes Compilation :

Important points to remember

1. Errors in data processing can be effectively detected with hash totals.
2. An integrated test facility can create fictitious data in the database to test the transaction process capability while the database in the production mode. Therefore, if you use integrated testing facility you do not have to setup separate test process. However, you have to be careful that the test data do not mix up with the production data.
3. An IS auditor should report all his reportable findings in his final report including those that have been corrected by the auditee immediately after the identification during the audit period. If the finding is corrected before the audit ends, the auditor should mention about the corrective action in his report.
4. A risk assessment always expects to identify the vulnerabilities and the threats.
5. The actual state of a system is compared to the expected or ideal state in a gap analysis process.
6. If there is any disagreement about the impact of an audit finding between the auditor and the auditee, then the auditor should explain the risks and the potential exposures to the auditee. An auditee may lack the required knowledge and understanding to realize the seriousness of a threat or risk.
7. If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposure since the auditee may not fully appreciate the magnitude of the

exposure. When the auditee expresses an alternative view, the auditor should not agree with him but he should communicate maintaining his professional code of conduct.

8. The main reason to have a control self-assessment (CSA) is help the internal audit function. This is achieved by transferring some control monitoring responsibilities to the line managers. Therefore, the success of CSA depends much on how the line managers handle their control monitoring responsibility.

9. The audit hook is the most effective online audit monitoring technique used for early detection of irregularities and errors.

10. Addressing the audit objectives is the primary goal of an IS auditor during the planning phase of an audit.

11. At the time of assessing network-monitoring control, an auditor needs to check, at first, the network documentation such as network topology.

12. Before formally closing a review, an IS auditor needs to meet the auditee to get agreement on his findings.

13. It is the IS auditor who decides whether to include a finding in the final report or not, not the auditee or anyone else.

14. During an investigation phase, if an IS auditor suspect the presence of fraudulent activity then he should decide whether he should gather further indication of the fraud. The auditor should inform the auditee only if he thinks that he has sufficient indicators or evidence of fraud. Generally, an IS auditor is not authorized to consult with legal authority external to the organization.

15. An audit charter describes the role of IS audit function. It also must specify the authority, responsibilities and scope of the audit function. A charter need to be approved by the top management and the audit committee.

16. An engagement letter states the scope and objectives, which has been agreed by both the auditor and the auditee.
17. Compliance test on change management process will reveal that whether any unauthorized modification was made to data or programs.
18. Continuous auditing and continuous monitoring is not the same thing. IS management provides continuous monitoring with a set of tools, mostly are automated, to meet fiduciary objectives. Examples of the tools used for continuous monitoring are IDS, antivirus etc.
19. What is continuous auditing? It is a methodology that an IS auditor uses to give written assurance, which may be a series of reports, on a specific subject. The IS auditor provides these reports either when a specific event occurs or after a short time of that event.
20. Continuous assurance= continuous monitoring+ continuous auditing.

Important points to remember
1. Errors in data processing can be effectively detected with hash totals.
2. An integrated test facility can create fictitious data in the database to test the transaction process capability while the database in the production mode. Therefore, if you use integrated testing facility you do not have to setup separate test process. However, you have to be careful that the test data do not mix up with the production data.
3. An IS auditor should report all his reportable findings in his final report including those that have been corrected by the auditee immediately after the identification during the audit period. If the

finding is corrected before the audit ends, the auditor should mention about the corrective action in his report.

4. A risk assessment always expects to identify the vulnerabilities and the threats.

5. The actual state of a system is compared to the expected or ideal state in a gap analysis process.

6. If there is any disagreement about the impact of an audit finding between the auditor and the auditee, then the auditor should explain the risks and the potential exposures to the auditee. An auditee may lack the required knowledge and understanding to realize the seriousness of a threat or risk.

7. If the auditee disagrees with the impact of a finding, it is important for an IS auditor to elaborate and clarify the risks and exposure since the auditee may not fully appreciate the magnitude of the exposure. When the auditee expresses an alternative view, the auditor should not agree with him but he should communicate maintaining his professional code of conduct.

8. The main reason to have a control self-assessment (CSA) is help the internal audit function. This is achieved by transferring some control monitoring responsibilities to the line managers. Therefore, the success of CSA depends much on how the line managers handle their control monitoring responsibility.

9. The audit hook is the most effective online audit monitoring technique used for early detection of irregularities and errors.

10. Addressing the audit objectives is the primary goal of an IS auditor during the planning phase of an audit.

11. At the time of assessing network-monitoring control, an auditor needs to check, at first, the network documentation such as network topology.

12. Before formally closing a review, an IS auditor needs to meet the auditee to get agreement on his findings.
13. It is the IS auditor who decides whether to include a finding in the final report or not, not the auditee or anyone else.
14. During an investigation phase, if an IS auditor suspect the presence of fraudulent activity then he should decide whether he should gather further indication of the fraud. The auditor should inform the auditee only if he thinks that he has sufficient indicators or evidence of fraud. Generally, an IS auditor is not authorized to consult with legal authority external to the organization.
15. An audit charter describes the role of IS audit function. It also must specify the authority, responsibilities and scope of the audit function. A charter need to be approved by the top management and the audit committee.
16. An engagement letter states the scope and objectives, which has been agreed by both the auditor and the auditee.
17. Compliance test on change management process will reveal that whether any unauthorized modification was made to data or programs.
18. Continuous auditing and continuous monitoring is not the same thing. IS management provides continuous monitoring with a set of tools, mostly are automated, to meet fiduciary objectives. Examples of the tools used for continuous monitoring are IDS, antivirus etc.
19. What is continuous auditing? It is a methodology that an IS auditor uses to give written assurance, which may be a series of reports, on a specific subject. The IS auditor provides these reports either when a specific event occurs or after a short time of that event.
20. Continuous assurance= continuous monitoring+ continuous

auditing.

21. The prerequisites for the success of continuous a
uditing depends on
the presence of automation and reliable automated process, alarms to notify control failures, automated audit tools for IS auditors, informing the IS auditor about system anomalies or errors, quick issuance of audit report, technical competency of auditors, reliable evidence, strictly following materiality guidelines, evaluation of cost factors.

22. The audit charter works as an instrument that delegates the audit authority to the IS audit function.

23. While developing a risk-based audit, the IS auditor is most likely to focus on business processes.

24. It is common that the same person taking part in system development and system maintenance.

25. IS strategic plan may include an analysis of the future business objectives.

26. The main benefit of having CSA (control self-assessment) in an organization is that it can identify that the high risk areas.

27. A compliance test always determines whether the controls are in place. An IS auditor testing that if the new accounts were properly authorized is an example of compliance test.

28. A substantive test always verifies the integrity of the system or application. Checking the balances of a financial statement is an example of substantive test.

29. The selection of audit procedures affects the detection risk. A faulty audit procedure may not identify the detection risk. That is why an IS auditor's decision can directly affect the detection risk.

30. When an IS auditor reviewing a SOA (service oriented application)

application, at first he needs to understand how the mapping of the business processes to services was done.

31. When an IS auditor discover the presence of authorized access requests that has not been authorized by the proper authority such as managers, he needs to conduct further analysis and substantive test to determine why the normal authorization process did not work. Before making any decision, an auditor should understand the context of the incident and collect sufficient evidence to support his action.

32. Attribute sampling can estimate the rate of occurrence of a specific attribute of quality in a population. That is why attribute sampling is used in compliance testing.

33. When there is not enough sample or data to draw from the population to make any assurance about the test objective, an IS auditor need to find an alternative approach of testing.

34. If an IS auditor is involved in the development, acquisition or implementation process of an application, then his independence will be impaired if he performs the post-implementation review of that application.

35. To establish accountability and responsibility of the processing of information or transaction is the main purpose of audit trail.

36. Identifying the high-risk areas is the most critical steps in audit planning.

37. The threats and vulnerabilities affecting the IT resources should be reviewed first when an IS auditor evaluate management's risk assessment of information system.

38. Audit's scope and purpose determines to what extent data will be collected as audit evidence.

39. The main objective of forensic software is to preserve digital

evidence.
40. When an IS auditor imports data from the database, he can make sure that the imported data are complete by checking the control totals of the original data to the imported data. To ensure completeness of data both the control totals should match.
41. Some of the important features of generalized audit software are statistical analysis, duplicate data checking, computation, mathematical computing and sequence checking.
42. During the audit phase, if an IS auditor discover that there is no documented security procedures in the organization, then he should try to identify and evaluate the security practices that the organization follow.
43. Among all types of evidence sources, the evidence collected from a reliable third party is considered the most reliable evidence.
44. The IS auditor should always be concerned on when the controls are applied as data pass through the system.
45. By observing and taking interviews an IS audito
r can get the best
evidence about the segregation of duties in an organization.
46. After review of any plan such as business continuity plan, an IS auditor need to call a meeting with the management to agree on the facts of his findings and to give them an opportunity to agree on the correction action.
47. IS auditors used data flow diagram to trace the data from its source to destination, highlighting data path and storage graphically.
48. An IS auditor considers a report from an external auditor more reliable than a confirmation letter to a third party. A confirmation letter does not follow any audit standards and is likely to be subjective.

49. An organization chart provides information about responsibility and authority of each person in an organization.
50. If an IS auditor discovers that the test resolute of a payment computation system do not match with his pre-determined totals, he should examine the cases where calculation mismatch occurred and need to confirm the results. The next step would be to conduct further test and to review the results.
51. The best way to determine the accuracy of a computing system is to make some simulated transaction and test the result with predetermined results.
52. If an auditor discovers some minor weaknesses in an application or in any system during an audit, he should record his observation and the risk that may arise by putting all the weakness together.
53. Developing audit plan based on risk assessment is the first step to ensure that audit resources deliver the highest value to the organization. That is why a risk assesment is perfromed during the planning phase of an audit to give reasonale asssurance that the audit will cover all the material items.
54. The validity of purchase order can be examined by testing the access control to the inventory application (testing of access control will reveal whether the appropriate person are modifying the application parameters.)
55. When the probability of errors need to be identified objectively, an IS auditor should use statistical sampling, not the judgmental/nonstatistical sampling.
56. Conducting a physical count of tape inventory is an example of substantive test.
57. If an IS auditor finds that the interview answers of a financial personal do not match with the job description for the role, then he

should conduct further testing with substantive test.
58. An IS auditor should never recommend any vendor product as a solution to the vulnerability in his audit report.
59. At the pre-audit phase, an IS auditor performs functional walkthrough in order understand the business processes.
60. An automated code comparison will reveal the presence of unauthorized changes in program since the last authorized program changes and update.
61. The audit report should be supported by sufficient and relevant audit evidence.
62. If an IS auditor find indication that the auditee is using unlicensed software, he should gather sufficient evidence before including his findings in the audit report.
63. An IS auditor always need to gather appropriate and sufficient evidence in order to provide a strong base for his conclusion on the audit findings.
64. The first step of evaluating the logical access control is to understand the security risk to the information processing. The second step is to document the controls that are applied to the logical access control path. In the third step, a test is conducted to determine whether the controls are functioning. In the last step, an IS auditor evaluates the existing policy and practices and compare them to the best practices in the industry.
65. A reboot in the system can destroy all the evidence of a compromised computer.
66. The main purpose of forensic audit is to systematically collect digital evidence to use in judicial proceedings.
67. When an IS auditor evaluate data mining and audit software that he want to utilize in his audit, he should ensure that this audit software

tool maintains data integrity and do not modify the system or its source code.

68. Conversation and interviews provides the best evidence that segregation of duties exist in an organization.

69. Testing of users rights provides incomplete information about the function they perform in their job role; it only provides information about the rights the users have in the IS systems.

70. An IS auditor shouold not recommed any specific vendor product in his audit report. If he does so, it ill compromise his professional independence.

71. To Identify and to evaluate the existing best practices is what an IS auditor needs to do when he finds no documented security procedures during an audit.

72. In a meeting that takes place after conducting an audit on disaster recover plan, the IS auditor should confirm the accuracy of his findings with the management.

73. Before submitting the audit report an auditor should ensure if the audit has sufficient evidence to support the findings.

74. Generalized audit software(GAS) is best suited to conduct overpayment audits because GAS has the ability to run statistical analysis, duplicate checking, sequencing, recomputation and various types of mathematical computation.

75. When an IS auditor needs to run further testing before gaining enough assurance in his audit, but cannot run the test due to limited time frame of the audit, he should highlight this in his report. Besides, a follow-up testing date should be scheduled.

76. An IS auditor is responsible for making the final decision on whether to include a material finding in the audit report or not.

77. Replacing a manual monitoring process with automated monitoring system can reveal the presence of overlapping key controls in application systems.
78. When assessing the risk of the information systems, the key factor that an IS auditor should, at first, review is the vulnerabilities and threats that may affect the IS assets.
79. To check the accuracy of a tax calculation system, you can simulate a transaction processing and then compare the result with precalcuated one.
80. Project management skills help an auditor to understand the constraints of performing an audit.
81. During the audit period, if the auditor detect the presence of virus or any malicious programs, he should inform the appropriate staff.
82. To objectively quantify the probability of errors, an IS auditor should use statistical sampling, not judgmental.
83. By running an automated code comparison, an auditor can detect the presence of unauthorized program modification.
84. While reviewing an application control, an IS auditor should focus on the automated controls of the application, and the potential exposure that may occur due to the weakness of the controls.
85. During the review process of sensitive electronic data, if an IS auditor find that the data are not encrypted, he may conclude that the data might have been compromised.
86. The first step to make sure that the audit resources returns best value to the organization is to plan an audit based on risk assessment.
87. When an IS auditor discovers the presence of a IT device that is missing in the diagram that he is using to plan the audit, he should immediately assess the impact of that device in the audit. If an

undocumented IS system or asset do not impact the audit scope, it can be eliminated from the audit.

88. A validity check helps to evaluate the password verification process because it checks if the required format is being used in the password,

89. During an audit, if an auditor finds out that user account ID of a website is being shared, he should document the finding in his report, explaining the risk of using shared IDs.

90. When an IS auditor extract data directly from a system for analysis, his action gives more assurance to data validity than IT personals performing the extraction. The main risk of IT personal extracting data is that they can filter out the exceptions that the IT auditor may need to examine to complete the audit.

91. When an organization decides to upgrade its database, an auditor should not advise on the efficiency of the upgrade, software licensing cost esitmation and application controls because all of these
actions compromise the auditor's independence. He can only review the acceptance test document of the database before carrying out the actual test.

92. The management is suspecting fraudulent transaction, and requested an auditor to review the transaction. In this case, the primary focus of the IS auditor should be to maintain the integrity of the evidence.

93. During an audit, an auditor discover that the same person is responsible for both IT and accounting. The review of computer log showing individual transaction would work as the best compensating control in this situation.

94. The main objective of an auditor discussing the audit findings with

the auditee is to confirm the accuracy of the findings, and to decide on the corrective actions required to fix the vulnerabilities.

95. After interviewing the IS staff, if an IS auditor finds that the job description does not match with the answer, he should expand the scope of his audit, and may think of conducting substantive testing.

96. To detect the presence of duplicate invoice record, an IS auditor can use Computer Aided Audit Techniques (CAATs).

97. During an audit an IS auditor discover that one of his associate had implemented the system that is under his audit scope. In this scenario, the auditor need to disclose the issue to his client and continue his audit.

98. If an IS auditor get involved in dispute with an department manager over the audit findings, at first he should revalidate his findings.

99. An effective technique to identify the violation of segregation of duties in a new ERP system is to develop a program that can detect the conflicts in authorization.

100. When an IS auditor evaluate the combined effect of the three types of controls-preventive, detective and corrective- he should aware of the points where these controls are used when data pass through the system.

101. After identifying the business processes to be audited, the next step is to find out the control objectives and the activities that need to be validated in the audit.

102. When conducting an compliance test on sensitive data (e.g. personal information of customers) on an online system, the IS auditor should review the legal and regulatory requirements for data privacy.

103. An IS auditor need to use his professional judgment when selecting audit procedures to make sure that he collects sufficient evidence.

104. Trends and variation detection tools help to analyze audit trail in server to detect anomalies in both user behaviour and system behavior.
105. Walk through, which involves both inquiry and inspection, is the an effective way to assess the effectiveness of design controls of automated process such as billing process.
106. A compliance test helps an IS auditor to determine whether new accounts are being properly authorized. If an compliance test demonstrates that sufficient internal controls exists in the authorization process, then the auditor can minimize the level of substantive test.
107. A substantive test can reveal whether the operational controls of transaction processing is effective or not.
108. Addressing audit objectives is the primary goal of an IS auditor during the audit planning stage.
109. When an IS auditor discover threats and its potential impacts, he needs to identify and evaluate the existing controls.
110. To determine if there is any unauthorized modification of production data, the IS auditor need to review the change management process. A compliance test can detect that if the change management process are being applied consistently.
111. If the audit department develop and maintain an script for continuous auditing, and give it to the IT department for continuous monitoring, the IT department should continue using the script and it will not result in any compromise in professional independence of the audit team.
112. When an IS auditor discovers an performance issue in a network, the next step he should follow is to examine the network topology diagram to find out the points of network bottlenecks and othe

relevant details.

113. An auditor need to use "discovery" sampling method when he needs to find out whether a particular incidents such as fraud has taken place or not.

114. A risk can be shared by transferring it. Example of a risk transfer is taking an insurance policy.

115. To proactively detect emerging risk in large volume of transaction you need to use "continuous auditing" technique, which feeds realtime data to management so as a quick corrective action can be taken soon after the detection of any anomalies.

116. While reviewing the effectiveness of system generated exception report, an auditor need to review, at least, one sample of exception report and the follow-up actions. The responsible staff perform the follow-up action after the exception is discovered.

117. The first step before creating a risk ranking is to define the audit universe, which takes into account of organizational structure, authorization matrix and IT strategic plan.

118. Attribute sampling, used in compliance testing, can effectively determine whether a purchase order has been authorized according to authorization matrix.

119. If the number of incidents, while reviewing a change control procedures, is not high enough to draw reasonable conclusion, the IS auditor need to find an alternative testing procedure. In other words, every test has a minimum sample size target, if the sample size target could not be met, the auditor need to use alternative test.

120. While undertaking an audit, if the auditor suspects that an attack or any suspicious activity is going on, at first he should inform the management about the incident.

121. The account list generated by the system, with access levels, is considered as a reliable source of evidence to an auditor who is testing employee access to a system.

122. When developing audit plan an auditor need to identify the highestrisk system and plan the audit accordingly. The auditor should never rely on the report of the previous year's audit plan since it may not have been designed on risk-based audit approach.

123. The main advantage of continuous auditing is that it improves security of time-sharing system that process large number of transactions.

124. Computer jobs schedules overridden by operators can lead to unauthorized data modification, and it should be regarded as a control concern to an auditor.

125. Evidence obtained directly by the auditor is always considered more reliable than that provided by the system administrator or management.

126. Since an auditor remains directly involved in the process of collecting evidence using CAAT(computer assisted audit techniques), the audit report can focus more on the reliability of the data. The reliability of information source always reinforce the audit findings.

Spyware is a program that picks up information from PC drives by making copies of their contents.

Trojan horses are malicious or damaging code hidden within an authorized computer program. Hackers use Trojans to coordinate distributed denial-of-service (DDoS) attacks that overload a site so that it may no longer be able to process legitimate requests.

Any weakness noticed should be reported, even if it is outside the scope of the current audit. Weaknesses identified during the course of an application software review need to be reported to management.

To ensure synchronization and protection of the source and object, the source code should be moved first into an access-protected library before compiling. The best control would be provided by having the production control group copy the source program to the production libraries and then compile the program. This would ensure synchronization of the source and object code.

Function point analysis (FPA) is a technique for determining the size of a development task based on the number of function points. Function points are factors such as inputs, outputs, inquiries and logical internal files. While this will help determine the size of individual activities, it will not assist in determining project duration because there are many overlapping tasks.

A program evaluation review technique (PERT) chart will help determine project duration once all the activities and the work involved with those activities are known.

The basis for an expert system is the capture and recording of the knowledge and experience of individuals in an organization. This will allow other users to access information formerly held only by experts.

Replay Attack: Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access.

PRIYA'S NOTES

•Application testers should be restricted to the non production environment if they full access to production environment confidentiality integrity availability of data becomes questionable

•Performing a web application securreview is a necessary effort that would uncover security vulnerabilities that could be exploited by gac

•Hackers

In peer to peer computing the greatest concern is data leakage. More priority than virus infection and network performance issues

•Vpn is a mature technology they are hard break. But if remote access is enabled malicious code in a remote client can spread to organisation network

•One problem is when the vpn terminates inside the network and encrypted vpn traffic goes through firewall. This means firewall cannot adequately examine the traffic

•Transaction monitoring reduces the risk of loss due to fraudulent online payment systems

•Two factor authentication can be circumvented through Man in the middle attack

•A directory server in Pki makes other certificate available to users

•Hackers use Trojan horse to coordinate DDOS

•Proper location of IDs in network architecture is the first stepduring installation

•Blowfish algorithm is an encryption technique and it consume too much processing power

•SSL uses symmetric key for message encryption.. it is useful for block transmission

•To prevent Ip spoofing attack a firewall is configured to drop a packet of the source routing field is enabled

•Session border controllers enhance the security in access network. They hide real address and provide a public address. They hide network topology and users real address . They can also used to monitor bandwidth and quality of service. It can be used to protect Voip against Ddos

•In Voip DDos attack is a major concern

•Email filtering best one Bayesian it applies statistical modelling to messages by performing a frequency analysis in each word within the message and then evaluating the message as a whole.therefore it can ignore a suspicious keyword if the entire message is within normal bounds.

•Heuristic filtering or rule based is less effective because new exception rules may need to be defined when a valid message is labelled as spam.

•Signature based filtering is not useful for variable length messages

•Pattern matching is actually a degraded rule based techniques where rules operate at word level using wildcards and not at higher level

•What is a Zero-Day Vulnerability?

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users. In order for the vendor to rectify the vulnerability, the software company must release a patch.

•In case of bank wire transfer procedures data integrity is a major concern.

•Sql injection attack is best prevented by using built in validation

•The best defense against Trojan horse software is virus scanning software

•What is keystroke logger
It is a type of malware which send confidential information back to the attacker

•Defence in depth means using different security mechanisms that back each other up. E.g. using a firewall as well as logical access control on the host to control incoming network traffic

•Data owner formally authorise access. Data custodian implement information security within application and access rules to data and program. Security administrator implement physical and logical security of data

•Data diddling presents inherent risk. Reduced by compensating controls

•Data diddling involves changing data before they are entered into system

•Brute force attack _against password

•Ping of death_ DDos

•challenge-response system is a program that replies to an e-mail message from an unknown sender by subjecting the sender to a test (called a CAPTCHA) designed to differentiate humans from automated senders. The system ensures that messages from people can get through and the automated mass mailings of spammers will be rejected. Once a sender has passed the test, the sender is

added to the recipient's whitelist of permitted senders that won't have to prove themselves each time they send a message.

•DNS hijacking is a process in which an individual redirects queries to a domain name server (DNS). It may be accomplished through the use of malicious software or unauthorized modification of a server. Once the individual has control of the DNS, they can direct others who access it to a web page that looks the same, but contains extra content such as advertisements. They may also direct users to pages containing malware or a third-party search engine.

•Use of shared login credentials makes accountability impossible. This is especially a risk with privileged accounts

•When an IS auditor reviewing a LAN performance in an organisation should first examinedata voice and video throughput requirements.
Then network topology

•FTP is considered an insecure protocol. It passes login details in clear text and the hacker captures the login data could login in and download files on FTP server.

•Malicious code Trojan horse brute force attack and password cracking tools commonly attempts to log on to administrator account

1) The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a facilitator.

2) Using a statistical sample to inventory the tape library is an example of a

substantive test.

3) Audit responsibility enhancement is an objective of a control self-assessment (CSA) program.

4) If proper identification and authentication are not performed during access control, no accountability can exist for any action performed.

5) IS auditors are most likely to perform compliance tests of internal controls if, after their initial evaluation of the controls, they conclude that control risks are within the acceptable limits. Think of it this way: If any reliance is placed on internal controls, that reliance must be validated through compliance testing. High control risk results in little reliance on internal controls, which results in additional substantive testing.

6) In planning an audit, the most critical step is identifying the areas of high risk.

7) Prior audit reports are considered of lesser value to an IS auditor attempting to gain an understanding of an organization's IT process than evidence directly collected.

8) When evaluating the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of the point at which controls are exercised as data flows through the system.

9) The primary purpose of audit trails is to establish accountability and responsibility for processed transactions.

10) When implementing continuous monitoring systems, an IS auditor's first step is to identify high-risk areas within the organization.

11) Auditing resources are allocated to the areas of highest concern, as a benefit of a risk-based approach to audit planning.

12) Inherent risk is associated with authorized program exits (trap doors).

13) After an IS auditor has identified threats and potential impacts, the auditor should identify and evaluate the existing controls.

14) Generalized audit software can be used to search for address field duplications.

15) The use of statistical sampling procedures helps minimize detection risk.

16) Lack of reporting of a successful attack on the network is a great concern to an IS auditor.

17) Detection risk results when an IS auditor uses an inadequate test procedure and concludes that material errors do not exist when errors actually exist.

18) An integrated test facility is considered a useful audit tool because it compares processing output with independently calculated data.

A project sponsor is typically the senior manager in charge of the primary business unit that the application will support.

The sponsor provides funding for the project and works closely with the project manager to define the critical success factors or metrics for the project.

The project sponsor is not responsible for reviewing the progress of the project.

A project steering committee that provides an overall direction for the enterprise resource planning (ERP) implementation project is responsible for reviewing the project's progress to ensure that it will deliver the expected results.

To ensure the effectiveness of controls, it is most effective to conduct re-performance. When the same result is obtained after the performance by an independent person, this provides the strongest assurance.

The restore window is the amount of time taken to recover the data. Because these are compliance-related backup data and are not being used for production, this is less critical than reliability.

Blind testing is also known as black-box testing.

This refers to a test where the penetration tester is not given any information and is forced to rely on publicly available information. This test simulates a real attack, except that the target organization is aware of the test being conducted.

Targeted testing is also known as white-box testing.

This refers to a test where the penetration tester is provided with information and the target organization is also aware of the testing activities. In some

cases, the tester is also provided with a limited-privilege account to be used as a starting point.

Double-blind testing is also known as zero-knowledge testing.

This refers to a test where the penetration tester is not given any information and the target organization is not given any warning—both parties are “blind” to the test.

This is the best scenario for testing response capability because the target will react as if the attack were real.

External testing refers to a test where an external penetration tester launches attacks on the target’s network perimeter from outside the target network (typically from the Internet).

Database integrity checks are important to ensure database consistency and accuracy. These include isolation, concurrency and durability controls.

Atomicity—the requirement for transactions to complete entirely and commit or else roll back to the last known good point.

Database commits ensure that the data are saved after the transaction processing is completed.

Rollback ensures that the processing that has been partially completed as part of the transaction is reversed back and not saved, if the entire transaction does not complete successfully.

The most effective method of rendering data irrecoverable is physical destruction of the storage media. Running a low-level data wipe utility may leave some residual data that could be recovered. Erasing data directories is easily reversed, exposing all data on the drive to unauthorized individuals.

The planning stage of the IS department should specifically consider the manner in which resources are allocated in the short-term.

Investments in IT need to be aligned with top management strategies, rather than focusing on technology for technology's sake.

Conducting control self-assessments and evaluating hardware needs are not as critical as allocating resources during short-term planning for the IS department

==========

The data control department performing data entry is responsible for receiving source documents from various departments and ensuring proper safekeeping of such until processing is complete and source documents and output are returned.

The IS Auditor's first and foremost responsibility is to advise senior management of the risk involved in having the security
administrator perform an operations function. This is a violation of separation of duties.

Three concepts are used to create a level of fault tolerance and redundancy in transaction processing.

They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level.

Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due

to inadvertent or malicious alterations to user or system data.

Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.

There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.

==========

Low equal error rate (EER) is a combination of the low false rejection rate and the low false acceptance rate.

EER,
expressed as a percentage, is a measure of the number of times that the false rejection and false acceptance are

equal.

A low EER is the measure of the more effective biometrics control device.
Low false rejection rates or low false acceptance rates alone do not measure the efficiency
of the device. Estimated error rate is non-existing and hence irrelevant.

Implementing database definition controls is one of the primary functions of the database administrator.

==========

Security administrators are generally held responsible for day-to-day network security operations, while also balancing security operations with overall network performance. This may include managing user accounts, implementing security patches and other related system software upgrades, writing scripts for routinely archiving log files to a centralized secured
server set up for this purpose and managing the systems workload to maintain performance within acceptable thresholds.
Security administrators are responsible for assuring that management policies and procedures are implemented on all systems,

participating with senior system administrators in the development of standard system "builds" and monitoring on

A sound IS security policy will most likely outline a response program to handle suspected intrusions.