CISA Certified Information Systems Auditor Practice Exams

By Peter H. Gregory

Governance and Management

Questions and Answers

1. Management's control of information technology processes is best described as
   Information technology governance
2. What is the best method for ensuring that an organization's IT department achieves adequate business alignment?
   Understand the organization's vision, mission statement, and objectives.
3. Roberta has located her organization's mission statement and a list of strategic objectives. What steps should Roberta take to ensure that the IT department aligns with the business?
   Discuss strategic objectives with business leaders to better understand what they wish to accomplish and what steps are being taken to achieve them.
4. Michael wants to improve the risk management process in his organization by creating content that will help management understand when certain risks should be accepted and when certain risks should be mitigated. The policy that Michael needs to create is known as
   A risk appetite statement
5. In a typical risk management process, the best person to make a risk treatment decision is
   The department head associated with the risk
6. The ultimate responsibility for an organization's cybersecurity program lies with
   The board of directors
7. In a US public company, a CIO will generally report the state of the organization's IT function to
   The board of directors
8. A new CIO in an organization is building its formal IT department from the ground up. In order to ensure collaboration among business leaders and department heads in the organization, the CIO should form and manage:
   An IT steering committee
9. The best person or group to make risk treatment decisions is

The cybersecurity steering committee

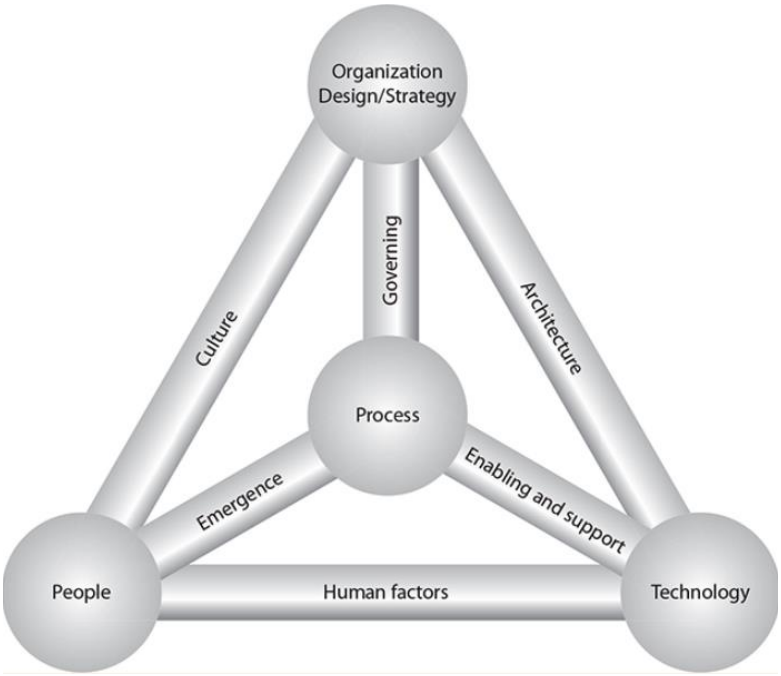
10. Which is the best party to conduct access reviews?
    Department head
11. Which is the best party to make decisions about the configuration and function of business applications?
    Business department head
12. Which of the following is the best definition of custodial responsibility?
    The custodian makes decisions based on the customer's defined interests.
13. What is the primary risk of IT acting as custodian for a business owner?
    IT may have insufficient knowledge of business operations to make good decisions.
14. An organization needs to hire an executive who will build a management program that considers threats and vulnerabilities. The best job title for this position is
    CRO Chief Risk Officer
15. An organization needs to hire an executive who will be responsible for ensuring that the organization's policies, business processes, and information systems are compliant with laws and regulations concerning the proper collection, use, and protection of personally identifiable information. What is the best job title for the organization to use for this position?
    Chief Privacy Officer (CPO)
16. The Big Data Company is adjusting several position titles in its IT department to reflect industry standards. Included in the consideration are two individuals: The first is responsible for the overall relationships and data flows among the company's internal and external information systems. The second is responsible for the overall health and management of systems containing information. Which two job titles are most appropriate for these two roles?
    Data architect and database administrator
17. What is the primary distinction between a network engineer and a telecom engineer?
    A network engineer is primarily involved with networks and internal network media (including cabling and internal wireless networks such as Wi-Fi), whereas a telecom engineer is primarily involved with networks and external (carrier) network media such as MPLS, Frame relay and dark fiber.
18. An organization that is a U.s public company is redesigning its access management and access review controls. What is the best role for Internal Audit in this redesign effort?
    Provide feedback on control design.
19. A security operations manager is proposing that engineers who design and manage information systems play a role in the monitoring of those systems. Is design and management compatible with monitoring? Why or why not?

Yes, Personnel who design and manage systems will be more familiar with the steps to take, as well as the reasons to take them, when alerts are generated.

20. The purpose of metrics in an IT department is to
    Measure the performance and effectiveness of controls.
21. Which security metric is best considered a leading indicator of an attack?
    Mean time to apply security patches
22. Steve, A CISO, has vulnerability management metrics and needs to build business-level metrics. Which of the following is the best business-level, leading indicator metric suitable for his organization's board of directors?
    Average time to patch servers supporting manufacturing processes
23. The metrics 'percentage of systems with completed installation of advanced anti-malware' is best described as
    A key goal indicator (KGI)
24. A member of the board of directors has asked Ravila, a CIRO, to produce a metric showing the reduction of risk as a result of the organization making key improvements to its security information and event management system. Which type of metric is most suitable for this purpose?
    KRI key risk indicator
25. A common way to determine the effectiveness of IT metrics is the SMART method. SMART stands for
    Specific, Measurable, Attainable, Relevant, Timely
26. The statement 'Complete migration of flagship system to latest version of vendor-supplied software' is an example of
    An objective statement
27. Ernie, a CIO who manages a large IT team, wants to create a mission statement for the team. What is the best approach for creating this mission statement?
    Start with the organization's mission statement.
28. Which of the following statements is the best description for the purpose of performing risk management?
    Identify and manage threats that are relevant to the organization.
29. Key metrics showing the effectiveness of a risk management program would not include
    *Reduction in the number of patches applie*d
30. Examples of security program performance metrics include all of the following except:
    Time to perform security scans
31. Two similar-sized organizations are merging. Paul will be the CIO of the new, combined organization. What is the greatest risk that may occur as a result of the merger?
    Differences in practices that may not be understood
32. The purpose of value delivery metrics is

Long-term reduction in costs

33. Joseph, a CIO, is collecting statistics on several operational areas and needs to find a standard way of measuring and publishing information about the effectiveness of his program. Which of the following is the best approach to follow?
    Balanced scorecard (BSC)
34. Which of the following is the best description of the Business Model for Information Security (BMIS)?
    Describes the relationships (as dynamic interconnections) between people, process, technology and the organization.
35. What is the correct name for the model shown here?



    Business model for information security
36. Jacqueline an experienced CISO, is reading the findings in a recent risk assessment that describes deficiencies in the organization's vulnerability management process. How would Jacqueline use the Business Model for Information Security (BMIS) to analyze the deficiency?

Identify the dynamic interconnections (DIs) connected to the process element.

37. Which of the following would constitute an appropriate use of the Zachman enterprise framework?
    IT systems described at a high level and then in increasing levels of detail.
38. An IT architect needs to document the flow of data from one system to another, including external systems operated by third-party service providers. What kind of documentation does an IT architect need to develop?
    Data flow diagrams (DFDs)

39. Carole is a CISO in a new organization with a fledgling security program. Carole needs to identify and develop mechanisms to ensure desired outcomes in selected business processes. What is a common term used to define these mechanisms?
    Controls
40. What is the best approach to developing security controls in a new organization?
    Start with a standard control framework and make risk-based adjustments as needed.
41. Which of the following is the best description of the COBIT framework?
    An IT process framework that includes security processes that are interspersed throughout the framework.
42. One distinct disadvantage of the ISO 27001 standard is
    The standard is costly
43. Which of the following statements about ISO 27001 is correct?
    ISO 27001 consists primarily of a body of requirements for running a security management program, along with an appendix of security controls.
44. The U.S. law that regulates the protection of data related to medical care is
    HIPAA Health Insurance Portability and Accountability Act
45. The regulation "Security and Privacy Controls for Federal Information Systems and Organizations" is better known as
    NIST SP800-53
46. What is the best explanation for the implementation of Tiers in the NIST Cybersecurity Framework?
    Implementation Tiers are likened to maturity levels.
47. Jeffrey is a CIO in an organization that performs financial services for private organizations as well as government agencies and U.S federal agencies. Which is the best information security controls framework for this organization?
    NIST 800-53
48. The scope of requirements of PCI-DSS is
    All systems that store, process and transmit credit card numbers, as well as all other systems that can communicate with these systems.
49. Which of the following statements is true about controls in the Payment Card Industry Data Security Standard?
    All controls are required, regardless of the actual risk.
50. The PCI-DSS is an example of
    A private industry standard that is enforced by contracts.
51. What are three factors that a risk manager might consider when developing an information security strategy?
    Risk levels, operating costs and compliance levels.
52. The responsibility for facilitation of an organization's cybersecurity program lies with

The chief information security officer (CISO)

The Audit Process

Questions and Answers

1. The IT Assurance Framework consists of all of the following except:
   ISACA Audit Job Practice
2. An Auditor is examining an IT organization's change control process. The auditor has determined that change advisory board (CAB) meetings take place on Tuesdays and Fridays, where planned changes are discussed and approved. The CAB does not discuss emergency changes that are not approved in advance. What opinion should the auditor reach concerning emergency changes?
   The Change Advisory Board should be discussing recent emergency changes.
3. A conspicuous video surveillance system would be characterized as what type(s) of control?
   Detective and deterrent
4. Michael is developing an audit plan for an organization's data center operations. Which of the following will help Michael determine which controls require potentially more scrutiny than others?
   Risk assessment of the data center
5. An organization processes payroll and expense reports in a SaaS-based environment to thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of audit should the organization undertake?
   Service provider audit
6. An audit project has been taking far too long and management is beginning to ask questions about its schedule and completion. This audit may be lacking
   Effective project management
7. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions. This type of sampling is known as
   Statistical sampling
8. An auditor is auditing an organization's user account request and fulfillment process. What is the first type of evidence collection the auditor will likely want to examine?
   Document review

9. A lead auditor is building an audit plan for a client's financial accounting system. The plan calls for periodic testing of a large number of transactions throughout the audit project. What is the best approach for accomplishing this?
   Develop one or more CAATs.
10. A lead auditor is building an audit plan for a client's financial transaction processing system. The audit will take approximately three months. Which of the following is the best approach for reporting audit exceptions to the audit client?
    Advise the client of exceptions as they are discovered and confirmed
11. Which of the following is true about ISACA Audit Standards and Audit Guidelines?
    ISACA Audit Standards are mandatory
12. An auditor is auditing an organization's identity and access management program. The auditor has found that automated workflows are used to receive and track access requests and approvals. However, the auditor has identified a number of exceptions where subjects were granted access without the necessary requests and approvals. What remedy should the auditor recommend?
    Monthly user access reviews
13. Why are preventive controls preferred over detective controls?
    Preventive controls stop unwanted events from occurring, while detective controls only record them.
14. For the purposes of audit planning, can an auditor rely upon the audit client's risk assessment?
    Yes, if the risk assessment was performed by a qualified external entity.
15. An organization processes payroll and expense reports in a SaaS-based environment to thousands of corporate customers. Those customers want assurance that the organization's processes are effective. What kind of audit should the organization undertake?
    SSAE18
16. An auditor is auditing an organization's system-hardening policy within its vulnerability management process. The auditor has examined the organization's system-hardening standards and wants to examine the configuration of some of the production servers. What is the best method for the auditor to obtain evidence?
    Capture screenshots from randomly selected servers during a walkthrough with the systems engineer.
17. An auditor is auditing the user account request and fulfillment process. The event population consists of hundreds of transactions, so the auditor cannot view them all. The auditor wants to view a random selection of transactions, as well as some of the transactions for privileged access requests. This type of sampling is known as
    Judgmental sampling

18. An auditor is auditing an organization's user account request and fulfillment process. An auditor has requested that the control owner describe the process to the auditor. What type of auditing is taking place?
    Walkthrough
19. An external audit firm is performing an audit of a customer's financial accounting processes and IT systems. While examining a data storage system's user access permissions, the staff auditor has discovered the presence of illegal content. What should the staff auditor do next?
    Inform his or her supervisor
20. A QSA auditor in an audit firm has completed a PCI-DSS audit of a client and has found the client to be non-compliant with one or more PCI-DSS controls. Management in the audit firm has asked the QSA auditor to sign off on the audit as compliant, arguing that the client's level of compliance has improved from prior years. What should the QSA auditor do?
    Refuse to sign the audit report as compliant
21. An organization wants to drive accountability for the performance of security controls to their respective control owners. Which activity is the best to undertake to accomplish this objective?
    Undergo control self-assessments (CSAs).
22. An auditor is evaluating a control related to a key card mechanism protecting a data center from unauthorized visitors. The auditor has determined that the key card control is ineffective because visitors often 'piggyback' their way into the data center. What detective control should be implemented to compensate for this control deficiency?
    A video surveillance system with 90-day content retention that records all entrances and exits from the data center.
23. A U.S based organization processes payroll and expense reports in a SaaS-based environment to thousands of corporate customers. Customers outside the United States want assurance that the organization's processes are effective. What kind of an audit should the organization undertake?
    ISAE3402
24. A QSA (PCI) audit firm has been commissioned by a large merchant organization to perform a PCI-DSS report on compliance (ROC). The audit firm has noted that the merchant's compliance deadline is less than one month away. What should the audit firm do next?
    Inform the merchant that the report on compliance cannot be completed on time and that an extension should be requested.
25. An audit is developing an audit plan for an accounts payable function. Rather than randomly selecting transactions to examine, the auditor wants to select transactions

from low, medium, and large payment amounts. Which sample methodology is appropriate for this approach?
Stratified sampling

26. A cybersecurity audit firm has completed a penetration test of an organization's web application. The final report contains two findings that indicate the presence of two critical vulnerabilities. The organization disputes the findings because of the presence of compensating controls outside of the web application interface. How should the audit proceed?
The audit firm should permit the customer to have some management comments included in the final report.
27. What is the objective of the ISACA audit standard on organizational independence?
The auditor's placement in the organization should ensure the auditor can act independently.
28. An auditor is auditing an organization's risk management process. During the walkthrough, the auditor asked the auditee to list all of the sources of information that contribute to the process. The auditee cited penetration tests, vendor advisories, non-vendor advisories, and security incidents as all of the inputs. What conclusion should the auditor draw from this?
The process is ineffective, as risk assessments apparently do not occur or contribute to the process.
29. The capability wherein a server is constituted from backup media is known as which type of control?
Recovery control
30. Prior to planning an audit, an auditor would need to conduct a risk assessment to identify high-risk areas in all of the following situations except for
A PCI 'report on compliance' audit
31. Which of the following audit types is appropriate for a financial services provider, such as a payroll service?
SSAE18
32. Which of the following is the best method for ensuring that an audit project can be completed on time?
Distribute a 'provided by client' evidence request list at the start of the audit.
33. An auditor is about to start an audit of a user account access request and fulfillment process. The audit covers a six-month period from January through June. The population contains 1,800 transactions. Which of the following sampling methodologies is best suited for this audit?
Request the first five transactions from each month in the audit period.

34. An auditor is auditing an organization's personnel onboarding process and is examining the background check process. The auditor is mainly interested in whether background checks are performed for all personnel and whether background check results lead to no-hire decisions. Which of the following evidence collection techniques will support this audit objective?
    Request the background check ledger that includes the candidates' names, results of background checks and hire/no-hire decisions.
35. An auditor wants to audit the changes made to the DBMS configuration of a financial accounting system. What should the auditor use as the transaction population?
    All of the changes made to the database.
36. A credit card payment processor undergoes an annual PCI report on compliance (ROC) audit. What evidence of a passing audit should the payment processor provide to merchant organizations and others?
    The signed attestation of compliance (AOC)
37. Which of the following statements about the ISACA Audit Guidelines is correct?
    ISACA Audit Guidelines are not required.
38. An external auditor is auditing an organization's third-party risk management (TPRM) process. The auditor has observed that the organization has developed an ISO-based questionnaire that is sent to all third-party service providers annually. What value-added remarks can the auditor provide?
    The process can be more efficient if the organization develops risk-based tiers to save time auditing low-risk vendors.
39. What is the difference between an SSAE18 Type I audit and an SSA18 Type II audit?
    A Type I audit is an audit of process design, whereas a Type II audit is an audit of process design and process effectiveness.
40. An auditor is auditing the payment systems for a retail store chain that has 80 stores in the region. The auditor needs to observe and take samples from some of the stores' systems. The audit client has selected two stores that are located in the same city as the store chain headquarters and two stores in a nearby town. How should the audit of the store locations proceed?
    The auditor should learn more about the stores' systems and practices before deciding what to do.
41. As a part of the audit of a business process, the auditor has had a discussion with the control owner, as well as the control operators, and has collected procedure documents and records. The auditor is asking internal customers of the business process to describe in their own words how the business process is operated. What kind of evidence collection are these discussions with internal customers?
    Corroborative inquiry

42. Three months after the completion of an audit, the auditor has contacted the auditee to inquire about the auditee's activities since the audit and whether the auditee has made any progress related to audit findings. What sort of communication is this outreach from the auditor?
    The auditor is a good audit partner and wants to ensure the auditee is successful.
43. According to ISACA Audit Standard 1202, which types of risks should be considered when planning an audit?
    Business risk
44. An IT service desk department that provisions user accounts changes that occurred in the prior month are checked against the list of corresponding requests in the ticketing system. This activity is known as
    A monthly provisioning review
45. An organization with video surveillance at a work center has placed visible notices on building entrances that inform people that video surveillance systems are in use. The notices are an example of
    Deterrent controls
46. An auditor is planning an audit of a financial planning application. Can the auditor rely on a recent penetration test of the application as a risk-based audit?
    Yes, the auditor can make use of the pen test, but a risk assessment is still needed.
47. Which of the following is the best example of a control self-assessment of a user account provisioning process?
    Reconciliation of all user account changes with approved requests in the ticketing system ensures that all such changes were requested and approved.
48. The proper sequence of an audit of an accounts payable process is
    Identify control owners, make evidence requests, perform walkthroughs, do corroborative interviews.
49. An auditor is auditing an accounts payable process and has found no exceptions. The auditor has decided to select additional samples to see whether any exceptions may be found. Which type of sampling is the auditor performing?
    Discovery sampling
50. Which of the following methods is best suited for an auditee to deliver evidence to an auditor during the audit of a background check process?
    Secure file transfer portal
51. An auditor has completed an audit, and the deliverable is ready to give to the audit client. What is the best method for delivering the audit report to the client?
    In person, in a close-out meeting
52. What are the potential consequences if an IS auditor is a member of ISACA and is CISA certified and violates the ISACA Code of Professional Ethics?

Loss of ISACA certifications

53. An auditor is auditing an accounts payable process and has discovered that a single individual has requested and approved several payments to vendors. What kind of an issue has the auditor found?
    A separation of duties issues.
54. An organization uses an automated workflow process for request, review, approval, and provisioning of user accounts. Anyone in the organization can request access. Specific persons are assigned to the review and approval steps. Provisioning is automated. What kind of control is the separation of duties between the review and approval steps?
    Preventive control
55. An auditor is planning an audit of a monthly terminated users review procedure. The auditor is planning to ask the auditee for a list of current user accounts in Active Directory, as well as a list of current employees and a list of terminated employees from Human Resources, so that the auditor can compare the lists. What kind of audit is the auditor planning to perform?
    Reperformance
56. An IT service desk manager is the control owner for the IT department change control process. In an audit of the change control process, the auditor has asked the IT service desk manager to provide all change control tickets whose request numbers end with the digit '6'. What sampling methodology has the auditor used?
    Statistical sampling
57. Au auditor firm is planning an audit of an organization's asset management records. For what reason would the auditor request a copy of the entire asset database from the DBA versus a report of assets from the owner of the asset process?
    Independence of the evidence provider
58. An auditor has delivered a Sarbanes-Oxley audit report containing 12 exceptions to the audit client, who disagrees with findings. The audit client is upset and is asking the auditor to remove any six findings from the report. A review of the audit findings resulted in confirmation that all 12 findings are valid. How should the auditor proceed? Explain to the auditee that the audit report cannot be changed.
59. An auditor has delivered a Sarbanes-Oxley audit report containing 12 exceptions to the audit client, who disagrees with findings. The audit client is upset and is asking the auditor to remove any six findings from the report in the exchange for a payment of $25,000. A review of the audit findings resulted in confirmation that all 12 findings are valid. How should the auditor proceed?
    The auditor should report the matter to his or her manager.
60. An auditor is auditing a change control process. During a walkthrough, the control owner described the process as follows: 'Engineers plan their changes and send an email

about their changes to the IT manager before 5 P.M on Wednesday. The engineers then proceed with their changes during the change window on Friday evening.' What, if any, findings should the auditor identify?
The change control process lacks review and approval steps.

61. An organization utilizes a video surveillance system on all ingress and egress points in its work facility; surveillance cameras are concealed from view, and there are visible notices. What type of control is this?
Detective control
62. Au auditor is selecting samples from records in the user access request process. While privileged access requests account for approximately 5 percent of all access requests, the auditor wants 20 percent of the samples to be requests for administrative access. What sampling technique has the auditor selected?
Stratified sampling
63. An auditor is auditing a change control process by examining change logs in a database management system and requesting change control records to show that those changes were approved. The auditor plans to proceed until the first exception is found. What sampling technique is being used here?
Discovery sampling

IT Life Cycle Management

Questions and Answers

1. What is the best reason for considering proof of concept?
The system being evaluated is too complex to evaluate in a walkthrough or by analyzing its specifications.
2. A formal process whereby the organization gathers all business and technical requirements and forwards them to several qualified vendors, who then respond to them, is called
Request for proposals (RFP)
3. An organization that wishes to acquire IT products or services that it fully understands should issue what kind of document?
Request for proposals (RFP)
4. Which SEI CMM maturity level states that there is some consistency in the ways that individuals perform tasks from one time to the next, as well as some management planning and direction to ensure that tasks and projects are performed consistently?
Repeatable
5. At what stage in the acquisition process should a project team develop requirements?

Prior to writing the test plan

6. All of the following are activities a project manager must perform to ensure a project is progressing in accordance with its plan except
   Designing and testing the system
7. During which phase of the infrastructure development life cycle are all changes to the environment performed under formal processes, including incident management, problem management, defect management, change management and configuration management?
   Maintenance
8. Which management processes cover the post-implementation phase of the SDLC?
   Change management and configuration management
9. Change management and configuration management are key to which phase of the SDLC?
   Maintenance
10. Which of the following is a formal verification of system specifications and technologies?
    Quality assurance testing (QAT)
11. All of the following are considerations when selecting and evaluating a software vendor except
    Source code languages
12. Which type of quality assurance method involves the users rather than IT or IS personnel?
    User acceptance testing (UAT)
13. All the following are considered risks to a software development project except
    Termination of the project manager
14. Analysis of regulations and market conditions normally takes place during which phase of the SDLC?
    Feasibility study
15. Which term describes a Scrum project and is a focused effort to produce some portion of the total project deliverable?
    Sprint
16. For what reason would an Internet-based financial application record the IP address of users who log in?
    This provides forensic information that can be used later.
17. In the context of logical access controls, the terms “subject” and “object” refer to
    “Subject” refers to the person who is accessing the data and “object” refers to the data being accessed.
18. In the context of logical access control, what does the term “fail closed” mean?

If an access control mechanism fails, access will be denied.

19. When would you design an access control to "fail open"?
    In the case of building access controls, which would need to permit evacuation of personnel in an emergency.
20. What are the three levels of the Constructive Cost Model (COCOMO) method for estimating software development projects?
    Basic, Intermediate and Detailed
21. The best source for requirements for an RFP project is
    The organization's own business, technical and security requirements
22. An organization wants to build a new application, but it has not yet defined precisely how end-user interaction will work. Which application development technique should be chosen to determine end-user interaction?
    Prototyping
23. A project manager regularly sends project status reports to executive management. Executives are requesting that statues reports include visual diagrams showing the project schedule and project-critical paths from week to week. Which type of chart should the project manager use?
    PERT
24. During which phase of the SDLC are functionality and design characteristics verified?
    Testing
25. Which kind of testing ensures that data is being formatted properly and inserted into the new application from the old application?
    Migration testing
26. Which entity commissions feasibility studies to support a business case?
    IT steering committee
27. What is the purpose of a configuration management database?
    Storage of every change made to system components
28. When is the best time for an organization to measure the business benefits of a new system?
    One year after implementation
29. Which of the following represents the components of the project in graphical or tabular form and is a visual or structural representation of the system, software, or application?
    Object breakdown structure (OBS)
30. Which type of tests will determine whether there are any failures or errors in input, processing or output controls in an application?
    Data integrity tests
31. Which quantitative method of sizing software projects is repeatable for traditional programming languages, but is not as effective with newer, nontextual languages?

Source lines of code (SLOC)

32. Which type of testing, usually performed by developers during the coding phase of the software development project, is used to verify that the code in various parts of the application works properly?
    Unit testing
33. An organization is considering acquiring a key business application from a small software company. What business provision should the organization require of the software company?
    Place source code in escrow
34. Which phase of the SDLC is continually referenced during the development, acquisition, and testing phases to ensure that the system is meeting the required specifications?
    Requirements definition
35. What is the purpose of the review process after each phase of the SDLC?
    To ensure that project deliverables meet the agreed-upon requirements

IT Service Management

Questions and Answers

1. A device that forwards packets to their destination based on their destination IP address is known as a
   Router
2. A security manager is planning to implement a first-time use of a vulnerability scanning tool in an organization. What method should the security manager use to confirm that all assets are scanned?
   Compare the scan results with the contents of the Configuration Management Database (CMDB)
3. Which of the following methods should be used to create a point-in-tie copy of a large production database?
   Storage system snapshot
4. All of the following protocols are used for federated authentication except
   WSDL
5. What is typically the most significant risk associated with end users being local administrators on their workstations?
   Malware can run at the highest privilege level
6. Which of the following persons is best suited to approve users' access to sensitive data in a customer database?
   Customer service manager

7. An organization is planning a new SaaS service offering and is uncertain about the resources required to support the service. How should the organization proceed?
   Build a working prototype and perform load tests.
8. What is the best definition of a problem in ITTL-based service management?
   The same incident that occurs repeatedly.
9. Which of the following is the best relationship between system security and the use of vulnerability scanning tools?
   Patching and hardening are performed proactively, and vulnerability scanning is used to verify their effectiveness.
10. A SaaS provider and a customer are having a dispute about the availability of service, quality of service and issue resolution provided by the SaaS provider. What type of legal agreement should the parties add to their contract to better define these problems and their resolution?
    Service level agreement
11. What is the purpose of a business impact analysis?
    It defines the most critical business processes.
12. An IT architect needs to increase the resilience of a single application server. Which of the following choices will least benefit the server's resilience?
    Redundant power supply
13. Which of the following backup schemes best protects an organization from ransomware?
    Storage system snapshots
14. A mail order organization wants to develop procedures to be followed in the event that the main office building cannot be occupied, so that customer orders can still be *fulfilled. What kind of plans does the organization need to develop?*
    Business continuity plan
15. The IT department is planning on implementing disaster recovery capabilities in some of its business systems. What means should be used to determine which applications require DR capabilities and to what level of recoverability?
    Business impact analysis
16. Which of the following is the most compelling reason for an organization to not automate its data purging jobs in support of data retention policies?
    Legal holds
17. Which of the following schemes is most likely to be successful for workstations used by a mobile workforce?
    Automated patching followed by a system restart that the end user can control

18. The IT department completed a data discovery assessment and found that numerous users were saving files containing sensitive information on organization wide readable file shares. Which of the following is the best remediation for this matter?
    Change the org-wide readable share to read-only for most users.
19. For which users or groups should the SQL listener on a database management system be accessible?
    For the application and DBA accounts only
20. An organization's financial accounting system crashes every Friday night after backups *have completed. In ITIL terms, what process should be invoked?*
    Problem management
21. The IT organization is investigating a problem in its change management process whereby many changes must be backed out because they could not complete or because verifications failed. Which is the best remedy for this situation?
    Required more rigorous testing in a test environment prior to scheduling changes in production.
22. Which language is used to change the schema in a database management system?
    Data definition language (DDL)
23. A DBA has been asked to limit the tables, rows or columns that are visible to some users with direct database access. Which solution would best fulfill this request?
    Create one or more views.
24. An organization's IT department developed DR capabilities for some business applications prior to a BIA being performed. Now that a BIA has been performed, it has been determined that some IT applications' DR capabilities exceed what is called for in the BIA and that other applications fall short. What should be done to remedy this?
    Change IT application DR capabilities to align with BIA.
25. What is the purpose of hot-pluggable drives in a storage system?
    Ability to replace drives while the storage system is still running
26. What is the primary purpose of data restoration testing?
    To ensure that backups are being performed
27. Which of the following should approve RTO and RPO targets?
    Senior business executives
28. An organization has developed its first-ever disaster recovery plan. What is the best choice for the first round of testing the plan?
    Walkthrough
29. Which of the following best describes the purpose of a hypervisor?
    It creates and manages virtual machines
30. Which of the following best fits the definition of a set of structured tables with indexes, primary keys, and foreign keys?

Relational database

31. An organization uses its vulnerability scanning tool as its de factor asset management system. What is the biggest risk associated with this approach?
    Network engineers could build new IP networks not included in the scanning tool's configuration
32. Which of the following systems should be used for populating the IT asset database in an elastic cloud environment?
    Hypervisor
33. What is a typical frequency for running a job that checks Active Directory for unused user accounts?
    Every 90 days
34. The system interface standard that includes process control, IPC and shared memory is known as
    POSIX
35. An environment consisting of centralized servers running end-user operating systems that display on users' computers is known as
    Virtual desktop infrastructure
36. A data privacy officer recently commissioned a data discovery exercise to understand the extent to which sensitive data is present on the company's world-readable file share. The exercise revealed that dozens of files containing large volumes of highly sensitive data were present on the file share. What is the best first step the data privacy officer should take?
    Investigate each instance to see whether any files are a part of business processes.
37. A new IT manager is making improvements in the organization's management of unplanned outages. The IT manager has built a new process where repeated cases of similar outages are analyzed to identify their cause. What process has the IT manager created?
    Problem management
38. A new IT manager is making improvements in the organization's management of detailed settings on servers and network devices. The process that IT manager has made is part of
    Configuration management.
39. A new IT manager is making improvements in the organization's management of detailed settings on servers and network devices. The process includes the creation of a repository for storing details about this information. This repository is known as
    A configuration management database
40. A new IT manager is making improvements to the organization's need to make its systems and devices more resilient to attacks. The IT manager should update

The system and device hardening standard

41. A customer of a SaaS provider is complaining about the SaaS provider's lack of responsiveness to resolve security issues. What portion of the contract should the customer refer to when lodging a formal complaint?
    Service level agreement
42. Computer code that is found within the contents of a database is known as a
    Stored procedure
43. An organization is starting its first-ever effort to develop a business continuity and disaster recovery plan. What is the best first step to perform in this effort?
    Business impact analysis
44. What is the purpose of connecting two redundant power supplies to separate electrical circuits?
    System resilience in case one electrical circuit fails
45. An IT organization is modernizing its tape backup system by replacing its tape library system with a storage array, while keeping its tape backup software system. What has the organization implemented?
    Virtual tape library
46. An IT organization is modernizing its tape backup system by sending data to a cloud storage provider. What has the organization implemented?
    E-vaulting
47. A city government department that accepts payments for water use has developed a procedure to be followed when the IT application for processing payment is unavailable. What type of procedure has been developed?
    Business continuity plan
48. A city government IT department has developed a procedure to be followed when the primary application for accepting water usage payments has been incapacitated. The procedure calls for the initiation of a secondary application in a different data center. What type of procedure has been developed?
    Disaster recovery plan
49. What is the most important factor to consider in the development of a disaster recovery plan?
    The safety of personnel
50. An SSD is most used as
    Secondary storage
51. The phrase "you can't protect what you don't know about" refers to which key IT process?
    Asset management
52. The SOAP (Simple Object Access Protocol) protocol is related to

The exchange of data through an API

53. Restricting USB attached storage on end-user workstations addresses all of the following except
    System capacity management
54. The primary purpose of a dynamic Data loss prevention (DLP) system is
    To control unauthorized movement of sensitive information
55. What is the suitability for the use of a SIEM to alert personnel of system capacity and performance issues?
    If syslog events are generated, use cases related to performance and capacity can be developed.
56. After analyzing events and incidents from the past year, an analyst has declared the existence of a problem. To what is the analyst referring to?
    A specific type of incident is recurring
57. A DBA has determined that it is not feasible to directly back up a large database. What is the best remedy for this?
    Export the database to a flat file and back up the flat file.
58. What is the feasibility of using the results of a BIA in the creation of a system classification plan?
    A BIA will indicate operational criticality of specific data that is associated with critical business processes.
59. A system engineer is reviewing critical systems in a data center and mapping them to individual electrical circuits. The engineer identified a system with two power supplies that are connected to the same plug strip. What should the engineer conclude from this?
    The two power supplies should not be connected to the same circuit.
60. An IT architect is proposing a plan for improving the resilience of critical data in the organization. The architect proposes that applications be altered so that they confirm that transactions have been successfully written to two different storage systems. What scheme has been proposed?
    Two-phase commit
61. A department has completed a review of its business continuity plan through a moderated discussion that followed a specific, scripted disaster scenario. What kind of review was performed?
    Simulation
62. What is the purpose of salvage operations in a disaster recovery plan?
    To identify the damage to, and recoverability of, critical equipment and assets.
63. Random Access Memory (RAM) is most used as
    Main storage

64. All the following are valid reasons for removing end users' local administrators privileges on their workstations except:
    To prevent the use of personal web mail
65. The primary mission of data governance is
    To control and monitor all uses of sensitive or critical information
66. Many of the backout plans in the records of a change control process simply read, "Reverse previous steps". What conclusion can be drawn from this?
    Backout plans are not as rigorous as they should be
67. The purpose of a business impact analysis (BIA) is primarily
    To determine process dependencies
68. The purpose for pre-writing public statements describing the impact, response and recovery from a disaster include all the following except
    Pre-written public statements are required by regulations.

Information Asset Protection

Questions and Answers

1. A new information security manager has examined the systems in the production environment and has found that their security-related configurations are inadequate and inconsistent. To improve this situation, the security manager should create a
   Hardening standard
2. Which US government agency enforces retail or organizations' information privacy policy?
   Federal Trade commission
3. While useful for detecting fires, what is one known problem associated with the use of smoke detectors under a raised computer room floor?
   False alarm due to the accumulation of dust
4. An organization is seeking to establish a protocol standard for federated authentication. Which of the following protocols is least likely to be selected?
   SOAP
5. What is one distinct disadvantage of the use of on-premises web content filtering?
   Mobile devices are unprotected when off-network
6. What is the purpose of data classification?
   To establish rules for data protection and use
7. Blockchain is best described as
   A list of records that are linked using cryptography
8. The private keys for a well-known web site have been compromised. What is the best approach for resolving this matter?

Add an entry to a CRL for the web site's SSL keys.

9. A web application stores unique codes on each user's system in order to track the activities of each visitor. What is a common term for these codes?
   Session cookie
10. The term 'virtual memory' refers to what mechanism?
    Main storage space that exceeds physical memory and is extended to secondary storage.
11. What is the effect of suppressing the broadcast of SSID?
    Network is not listed, but no difference in security
12. What is the purpose of record keeping in a security awareness training program?
    Users cannot later claim no knowledge of content if they violate policy.
13. An attack technique in which an attacker attempts to place arbitrary code into the instruction space of a running process is known as
    A buffer overflow attack
14. A security analyst who is troubleshooting a security issue has asked another engineer to obtain a PCAP file associated with a given user's workstation. What is the security analyst asking for?
    A copy of the network traffic to and from the workstation.
15. A development lab employs a syslog server for security and troubleshooting issues. The information security office has recently implemented a SIEM and has directed that all log data be sent to the SIEM. How can the development lab continue to employ its local syslog server while complying with this request?
    Direct servers to send their syslog data to the local server and to the SIEM.
16. The best time to assign roles and responsibilities for computer security incident response is
    While writing the incident response plan
17. Chain of custody is employed in which business process?
    Internal investigation
18. Canada's ITSG-33 is a similar to which standard?
    NIST SP800-53
19. The process of ensuring proper protection and use of PII is known as
    Privacy
20. A CIO is investigating the prospect of a hosting center for its IT infrastructure. A specific hosting center claims to have "N+1 HVAC Systems." What is meant by this term?
    The hosting center has one more HVAC system than is necessary for adequate cooling.
21. An organization has updated its identity and access management infrastructure so that users use their AD credentials to log in to the network as well as internal business applications. What has the organization implemented?
    Reduced sign-on

22. The primary advantage of a firewall on a laptop computer is
    Laptop computers are protected when outside the enterprise network.
23. An organization's data classification policy includes guidelines for placing footers with specific language in documents and presentations. What activity does this refer to?
    Document marking
24. What technique does PGP use to permit multiple users to read an encrypted document?
    Digital envelope
25. What feature permits enterprise users of Microsoft Outlook to digitally sign e-mail messages?
    AD PKI
26. A URL starting with http:// signifies what technology?
    SET, or Secure Electronic Transaction
27. A recent audit of an IT operation included a finding stating that the organization experiences virtualization sprawl. What is the meaning of this term?
    The process related to the creation of new virtual machines is not effective.
28. Reasons for placing all IoT-type devices on isolated VLANs include all of the following except
    Compatibility with IPv4
29. What is the best reason for including competency quizzes in security awareness training courses?
    It provides evidence of retention of course content.
30. In the context of information technology and information security, what is the purpose of fuzzing?
    To assess a program's resistance to attach via the UI.
31. An attacker who is attempting to infiltrate an organization has decided to employ a DNS poison cache attack. What method will the attacker use to attempt this attack?
    Send forged query replies to a DNS server.
32. What is the Unix command to dynamically view the end of a text log file?
    Tail –f
33. In the United States, what are organizations required to do when discovering child pornography on a user's workstation?
    Immediately contact law enforcement
34. An organization suspects one of its employees of a security violation regarding the use of their workstation. The workstation, a laptop computer that is powered down, has been delivered to a forensic expert. What is the first thing the expert should do?
    Photograph the laptop
35. Which of the following statements is true regarding the Payment Card Industry Data Security Standard (PCI-DSS)?

Organizations processing fewer than six million merchant transactions annually are usually permitted to provide annual self-assessments.

36. According to the European General Data Protection Regulation (GDPR), what is the requirement for organizations' use of a Data Protection Officer (DPO)?
    All organizations storing large volumes of EU citizen data are required to use a DPO.
37. What is the biggest risk associated with access badges that show the name of the organization?
    Someone who finds the badge may know where it can be used.
38. A user at work logs on to a web site that includes links to various business applications. Once the user logs on to the web site, the user does not need to log on to individual applications. What mechanism provides this capability?
    Single sign-on
39. What is the primary advantage of cloud-based web content filtering versus on-premises web content filtering:
    Off-network users are protected just as in-office users are.
40. An organization is investigating the use of an automated DLP solution that controls whether data files can be sent via e-mail or stored on USB drives based on their tags. What is the advantage of the use of tags for such a solution?
    Data files are automatically processed based on tags instead of their data content.
41. All of the following are appropriate uses of digital signatures except
    Verification of message confidentiality
42. The entity that accepts requests for new public keys in a KPI is known as the
    Registration authority (RA)
43. What method is used by a transparent proxy filter to prevent a user from visiting a site that has been blacklisted?
    User is directed to a "web site blocked" splash page.
44. In a virtualized environment, which method is the fastest way to ensure rapid recovery of servers at an alternative processing center?
    Copy snapshots of virtual machine images to alternative processing center storage system.
45. In an environment where users are not local administrators of their workstations, which of the following methods ensures that end users are not able to use their mobile devices as mobile Wi-Fi hotspots for circumventing network security controls such as web content filters and IPS?
    Create a whitelist of permitted Wi-Fi networks.
46. What is the most effective method for training users to more accurately detect and delete phishing messages?
    Conduct phishing tests and privately inform offenders of their mistakes.

47. An attacker has targeted an organization in order to steal specific information. The attacker has found that the organization's defenses are strong and that very few phishing messages arrive at end-user inboxes. The attacker has decided to try a watering hole attack. What first steps should the hacker use to ensure a successful watering hole attack?
    Determine which web sites are frequently visited by the organization's end users.
48. Which of the following techniques most accurately describes a penetration test?
    Security scan, followed by manual exploitation of tools and techniques.
49. A security analyst spends most of her time on a system that collects log data and correlates events from various systems to deduce potential attacks in progress. What kind of system is the security analyst using?
    SIEM
50. The general counsel is becoming annoyed with notifications of minor security events occurring in the organization. This is most likely due to
    Lack of a security incident severity scheme
51. A forensic investigator is seen to be creating a detailed record of artifacts that are collected, analyzed, controlled, transferred to others, and stored for safekeeping. What kind of written record is this?
    Chain of custody record
52. Which controls framework is suggested by the ISO/IEC 27001 standard?
    ISO/IEC 27002
53. The default principle in the European General Data Protection Regulation for marketing communications from organizations to citizens is
    Citizens are excluded until they explicitly opt in.
54. The primary purpose of a mantrap is
    To permit entry or exit of one authorized person at a time.
55. What is the purpose of locking a user account that has not been used for long periods of time?
    Reduction of the risk of compromised credentials
56. What is the best approach for implementing a new blocking rule in an IPS?
    Put the rule in learn mode and analyze the results.
57. A security leader needs to develop a data classification program. After developing the data classification and handling policy, what is the best next step to perform?
    Work with business departments to socialize the policy.
58. An organization wants to implement an IPS that utilizes SSL inspection. What must first be implemented so that IPS will function?
    A new root certificate must be pushed to all user workstations.
59. In what manner does a PKI support disk encryption on end-user workstations?

PKI stores decryption keys in the event, and the end user forgets their bootup password.

60. A browser contacts a web server and requests a web page. The web server responds with a status code of 200. What is the meaning of this status code?
    The request is valid and has been accepted
61. For what reason would an engineer choose to use a hosted hypervisor versus a bare-metal hypervisor?
    Features available only in a host operating system are required.
62. The laboratory environment of a pharmaceutical research organization contains many scientific instruments that contain older versions of windows and Linux operating systems that cannot be patched. What is the best remedy for this?
    Isolate the scientific instruments on a separate, protected network.
63. Which of the following is the best policy for a security awareness training course?
    Users are required to repeat modules when they fail competency quizzes.
64. Guessing that an intended victim has a particular online banking session open, an attacker attempts to trick the victim into clicking on a link that will attempt to execute a transaction on the online banking site. This type of an attack is known as
    Cross-site request forgery
65. Which of the following tools is considered a search engine that can be used to list vulnerabilities in devices?
    Shodan
66. All the following tools are used to detect changes in static files except
    Firesheep
67. Which of the following correctly describes the correct sequence for computer security incident response?
    Detect, initiate, evaluate, contain, eradicate, recover, remediate
68. Which of the following devices is needed for the creation of a forensically identical hard disk drive?
    Write blocker
69. Which of the following statements about NIST CSF is true?
    NIST CSF is a policy framework for cybersecurity
70. The 'right to be forgotten' was first implemented by
    General Data Protection Regulation (GDPR)
71. The term 'tailgating' most often refers to
    Personnel who follow others into a protected facility without authentication
72. A security manager in a large organization has found that the IT department has no central management of privileged user accounts. What kind of a tool should the security manager introduce to remedy this practice?
    Privileged Access Management (PAM) tools

73. A security analyst has determined that some of the OS configuration file alterations have taken place without proper authorization. Which tool did the security analyst use to determine this?
    File integrity monitoring (FIM)
74. An employee notes that a company document is marked 'confidential'. Is it acceptable for the employee to e-mail the document to a party outside the company?
    This cannot be determined without first consulting the data classification and handling policy.
75. An auditor has completed an audit of an organization's use of a tool that generates SSL certificates for its external web sites. The auditor has determined that key management procedures are insufficient, and that split custody of the key generation procedure is required. How might this be implemented?
    Of two engineers, each has one half of the password required to create a new certificate.
76. An organization that issues digital certificates recently discovered that a digital certificate was issued to an unauthorized party. What is the appropriate response?

Create a CRL entry.

77. Why is it important for a web session cookie to be encrypted?
    Parties that can observe the communication will not be able to hijack the session.
78. Why would a hypervisor conceal its existence from a guest OS?
    To avoid letting an intruder know that the OS is part of a virtualized environment.
79. How can an organization prevent employees from connecting to the corporate Exchange e-mail environment with personally owned mobile devices?
    Put the OWA server behind the firewall and VPN switch
80. What is the purpose of the Firesheep tool?
    It demonstrates the dangers of non-encrypted web sessions.
81. An organization is implementing a new SIEM. How must engineers get log data from systems and devices to the SIEM?
    Send them via syslog and Windows events.
82. What is the appropriate consequence of SOC operations declaring incidents that turn out to be false positives?
    Additional training to improve their incident-handling skills.