



isaca.prep4sure.cisa.v2019-01- 24.by.ashley.699q.vce

CISA

CISA

Certified Information Systems Auditor

Score: 800/1000

Version:

Time Limit: 120 Minutes

Exam A (699 questions)

Question 1

Which of the following attack redirects outgoing message from the client back onto the client, preventing outside access as well as flooding the client with the sent packets?

- ☐ Banana attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 2

What is the key distinction between encryption and hashing algorithms?

- ☐ Hashing algorithms ensure data confidentiality.
- ☐ Hashing algorithms are irreversible.
- ☐ Encryption algorithms ensure data integrity.
- ☐ Encryption algorithms are not irreversible.

Question 3

What often results in project scope creep when functional requirements are not defined as well as they could be?

- ☐ Inadequate software baselining
- ☐ Insufficient strategic planning
- ☐ Inaccurate resource allocation
- ☐ Project delays

Question 4

COBIT 5 separates information goals into three sub-dimensions of quality. Which of the following sub-dimension of COBIT 5 describes the extent to which data values are in conformance with the actual true value?

- ☐ Intrinsic quality
- ☐ Contextual and representational quality
- ☐ Security quality
- ☐ Accessibility quality

Question 5

A legacy payroll application is migrated to a new application. Which of the following stakeholders should be PRIMARILY responsible for reviewing and signing-off on the accuracy and completeness of the data before going live?

- ☐ IS auditor
- ☐ Database administrator
- ☐ Project manager
- ☐ Data owner

Question 6

ISO 9126 is a standard to assist in evaluating the quality of a product. Which of the following is defined as a set of attributes that bear on the existence of a set of functions and their specified properties?

- ☐ Reliability
- ☐ Usability
- ☐ Functionality
- ☐ Maintainability

Question 7

Which of the following layer of an enterprise data flow architecture does the scheduling of the tasks necessary to build and maintain the Data Warehouse (DW) and also populates Data Marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Warehouse management layer
- ☐ Data access layer

Question 8

In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

- ☐ Appliances
- ☐ Operating system-based
- ☐ Host-based
- ☐ Demilitarized

Question 9

Which of the following software development methodology uses minimal planning and in favor of rapid prototyping?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 10

In which of the following transmission media it is MOST difficult to modify the information traveling across the network?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 11

An IS auditor is performing an audit of a remotely managed server backup. The IS auditor reviews the logs for one day and finds one case where logging on a server has failed with the result that backup restarts cannot be confirmed. What should the auditor do?

- ☐ Issue an audit finding
- ☐ Seek an explanation from IS management
- ☐ Review the classifications of data held on the server
- ☐ Expand the sample of logs reviewed

Question 12

During an exit interview, in cases where there is disagreement regarding the impact of a finding, an IS auditor should:

- ☐ ask the auditee to sign a release form accepting full legal responsibility.
- ☐ elaborate on the significance of the finding and the risks of not correcting it.
- ☐ report the disagreement to the audit committee for resolution.
- ☐ accept the auditee's position since they are the process owners.

Question 13

An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?

- ☐ Nonavailability of an alternate private branch exchange (PBX) system
- ☐ Absence of a backup for the network backbone
- ☐ Lack of backup systems for the users' PCs
- ☐ Failure of the access card system

Question 14

Which of the following is the key benefit of control self-assessment (CSA)?

- ☐ Management ownership of the internal controls supporting business objectives is reinforced.
- ☐ Audit expenses are reduced when the assessment results are an input to external audit work.
- ☐ Improved fraud detection since internal business staff are engaged in testing controls
- ☐ Internal auditors can shift to a consultative approach by using the results of the assessment.

Question 15

What is/are used to measure and ensure proper network capacity management and availability of services?

- ☐ Network performance-monitoring tools
- ☐ Network component redundancy
- ☐ Syslog reporting
- ☐ IT strategic planning

Question 16

Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?

- ☐ Bottom up
- ☐ Sociability testing
- ☐ Top-down
- ☐ System test

Question 17

To install backdoors, hackers generally prefer to use:

- ☐ either Trojan horse or computer worm.
- ☐ either Tripwire or computer virus.
- ☐ either eavedropper or computer worm.
- ☐ either Trojan horse or eavedropper.
- ☐ None of the choices.

Question 18

Which of the following layer of an enterprise data flow architecture is concerned with transporting information between the various layers?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Application messaging layer
- ☐ Data access layer

Question 19

The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- ☐ prevent omission or duplication of transactions.
- ☐ ensure smooth data transition from client machines to servers.
- ☐ ensure that e-mail messages have accurate time stamps.
- ☐ support the incident investigation process.

Question 20

In a public key infrastructure (PKI), which of the following may be relied upon to prove that an online transaction was authorized by a specific customer?

- ☐ Nonrepudiation
- ☐ Encryption
- ☐ Authentication
- ☐ Integrity

Question 21

In a public key infrastructure (PKI), the authority responsible for the identification and authentication of an applicant for a digital certificate (i.e., certificate subjects) is the:

- ☐ registration authority (RA).
- ☐ issuing certification authority (CA).
- ☐ subject CA.
- ☐ policy management authority.

Question 22

Library control software restricts source code to:

- ☐ Read-only access
- ☐ Write-only access
- ☐ Full access
- ☐ Read-write access

Question 23

Establishing the level of acceptable risk is the responsibility of:

- ☐ quality assurance management.
- ☐ senior business management.
- ☐ the chief information officer.
- ☐ the chief security officer.

Question 24

When reviewing print systems spooling, an IS auditor is MOST concerned with which of the following vulnerabilities?

- ☐ The potential for unauthorized deletion of report copies
- ☐ The potential for unauthorized modification of report copies
- ☐ The potential for unauthorized printing of report copies
- ☐ The potential for unauthorized editing of report copies

Question 25

Which audit technique provides the BEST evidence of the segregation of duties in an IS department?

- ☐ Discussion with management
- ☐ Review of the organization chart
- ☐ Observation and interviews
- ☐ Testing of user access rights

Question 26

Security should ALWAYS be an all or nothing issue.

- ☐ True
- ☐ True for trusted systems only
- ☐ True for untrusted systems only
- ☐ False
- ☐ None of the choices.

Question 27

Neural networks are effective in detecting fraud because they can:

- ☐ discover new trends since they are inherently linear.
- ☐ solve problems where large and general sets of training data are not obtainable.
- ☐ attack problems that require consideration of a large number of input variables.
- ☐ make assumptions about the shape of any curve relating variables to the output.

Question 28

An IS auditor finds that, in accordance with IS policy, IDs of terminated users are deactivated within 90 days of termination. The IS auditor should:

- ☐ report that the control is operating effectively since deactivation happens within the time frame stated in the IS policy.
- ☐ verify that user access rights have been granted on a need-to-have basis.
- ☐ recommend changes to the IS policy to ensure deactivation of user IDs upon termination.
- ☐ recommend that activity logs of terminated users be reviewed on a regular basis.

Question 29

Function Point Analysis (FPA) provides an estimate of the size of an information system based only on the number and complexity of a system's inputs and outputs. True or false?

- ☐ True
- ☐ False

Question 30

Which of the following is a substantive test?

- ☐ Checking a list of exception reports
- ☐ Ensuring approval for parameter changes
- ☐ Using a statistical sample to inventory the tape library
- ☐ Reviewing password history reports

Question 31

Which of the following is a dynamic analysis tool for the purpose of testing software modules?

- ☐ Blackbox test
- ☐ Desk checking
- ☐ Structured walk-through
- ☐ Design and code

Question 32

A benefit of open system architecture is that it:

- ☐ facilitates interoperability.
- ☐ facilitates the integration of proprietary components.
- ☐ will be a basis for volume discounts from equipment vendors.
- ☐ allows for the achievement of more economies of scale for equipment.

Question 33

During the planning stage of an IS audit, the PRIMARY goal of an IS auditor is to:

- ☐ address audit objectives.
- ☐ collect sufficient evidence.
- ☐ specify appropriate tests.
- ☐ minimize audit resources.

Question 34

Which of the following encryption methods uses a matching pair of key-codes, securely distributed, which are used once-and-only-once to encode and decode a single message?

- ☐ Blowfish
- ☐ Tripwire
- ☐ certificate
- ☐ DES
- ☐ one-time pad
- ☐ None of the choices.

Question 35

Which of the following PBX feature supports shared extensions among several devices, ensuring that only one device at a time can use an extension?

- ☐ Call forwarding
- ☐ Privacy release
- ☐ Tenanting
- ☐ Voice mail

Question 36

Functionality is a characteristic associated with evaluating the quality of software products throughout their life cycle, and is BEST described as the set of attributes that bear on the:

- ☐ existence of a set of functions and their specified properties.
- ☐ ability of the software to be transferred from one environment to another.
- ☐ capability of software to maintain its level of performance under stated conditions.
- ☐ relationship between the performance of the software and the amount of resources used.

Question 37

A virtual private network (VPN) provides data confidentiality by using:

- ☐ Secure Sockets Layer (SSL)
- ☐ Tunneling
- ☐ Digital signatures
- ☐ Phishing

Question 38

Though management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should:

- ☐ include the statement of management in the audit report.
- ☐ identify whether such software is, indeed, being used by the organization.
- ☐ reconfirm with management the usage of the software.
- ☐ discuss the issue with senior management since reporting this could have a negative impact on the organization.

Question 39

An IS auditor should be aware of various analysis models used by data architecture. Which of the following analysis models depict data entities and how they relate?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Question 40

Which of the following is used to evaluate biometric access controls?

- ☐ FAR
- ☐ EER
- ☐ ERR
- ☐ FRR

Question 41

Which of the following is a function of an IS steering committee?

- ☐ Monitoring vendor-controlled change control and testing
- ☐ Ensuring a separation of duties within the information's processing environment
- ☐ Approving and monitoring major projects, the status of IS plans and budgets
- ☐ Liaising between the IS department and the end users

Question 42

As an outcome of information security governance, strategic alignment provides:

- ☐ security requirements driven by enterprise requirements.
- ☐ baseline security following best practices.
- ☐ institutionalized and commoditized solutions.
- ☐ an understanding of risk exposure.

Question 43

An IS auditor is evaluating management's risk assessment of information systems. The IS auditor should FIRST review:

- ☐ the controls already in place.
- ☐ the effectiveness of the controls in place.
- ☐ the mechanism for monitoring the risks related to the assets.
- ☐ the threats/vulnerabilities affecting the assets.

Question 44

A perpetrator looking to gain access to and gather information about encrypted data being transmitted over the network would use:

- ☐ eavesdropping
- ☐ spoofing.
- ☐ traffic analysis.
- ☐ masquerading.

Question 45

Which of the following method of expressing knowledge base consist of a graph in which nodes represent physical or conceptual objects and the arcs describes the relationship between nodes?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Question 46

Which of the following is the initial step in creating a firewall policy?

- ☐ A cost-benefit analysis of methods for securing the applications
- ☐ Identification of network applications to be externally accessed
- ☐ Identification of vulnerabilities associated with network applications to be externally accessed
- ☐ Creation of an applications traffic matrix showing protection methods

Question 47

A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- ☐ Most employees use laptops.
- ☐ A packet filtering firewall is used.
- ☐ The IP address space is smaller than the number of PCs.
- ☐ Access to a network port is not restricted.

Question 48

An IS auditor is reviewing a project to implement a payment system between a parent bank and a subsidiary. The IS auditor should FIRST verify that the:

- ☐ technical platforms between the two companies are interoperable.
- ☐ parent bank is authorized to serve as a service provider.
- ☐ security features are in place to segregate subsidiary trades.
- ☐ subsidiary can join as a co-owner of this payment system.

Question 49

Fourth-Generation Languages (4GLs) are most appropriate for designing the application's graphical user interface (GUI). They are inappropriate for designing any intensive data- calculation procedures. True or false?

- ☐ True
- ☐ False

Question 50

What is the first step in a business process re-engineering project?

- ☐ Identifying current business processes
- ☐ Forming a BPR steering committee
- ☐ Defining the scope of areas to be reviewed
- ☐ Reviewing the organizational strategic plan

Question 51

An organization can ensure that the recipients of e-mails from its employees can authenticate the identity of the sender by:

- ☐ digitally signing all e-mail messages.
- ☐ encrypting all e-mail messages.
- ☐ compressing all e-mail messages.
- ☐ password protecting all e-mail messages.

Question 52

In what way is a common gateway interface (CGI) MOST often used on a webserver?

- ☐ Consistent way for transferring data to the application program and back to the user
- ☐ Computer graphics imaging method for movies and TV
- ☐ Graphic user interface for web design
- ☐ interface to access the private gateway domain

Question 53

Which of the following testing method examines internal structure or working of an application?

- ☐ White-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 54

Which of the following provide(s) near-immediate recoverability for time-sensitive systems and transaction processing?

- ☐ Automated electronic journaling and parallel processing
- ☐ Data mirroring and parallel processing
- ☐ Data mirroring
- ☐ Parallel processing

Question 55

An advantage of a continuous audit approach is that it can improve system security when used in time-sharing environments that process a large number of transactions. True or false?

- ☐ True
- ☐ False

Question 56

Identify the WAN message switching technique being used from the description presented below:

“Data is routed in its entirety from the source node to the destination node, one hop at a time. During message routing, every intermediate switch in the network stores the whole message. If the entire network's resources are engaged or the network becomes blocked, this WAN switching technology stores and delays the message until ample resources become available for effective transmission of the message. “

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Question 57

Which of the following is the INCORRECT "layer - protocol" mapping within the TCP/IP model?

- ☐ Application layer – NFS
- ☐ Transport layer – TCP
- ☐ Network layer – UDP
- ☐ LAN or WAN interface layer – point-to-point protocol

Question 58

Following best practices, formal plans for implementation of new information systems are developed during the:

- ☐ development phase.
- ☐ design phase.
- ☐ testing phase.
- ☐ deployment phase.

Question 59

Which of the following translates e-mail formats from one network to another so that the message can travel through all the networks?

- ☐ Gateway
- ☐ Protocol converter
- ☐ Front-end communication processor
- ☐ Concentrator/multiplexor

Question 60

Which of the following ACID property in DBMS ensures that the concurrent execution of transactions results in a system state that would be obtained if transactions were executed serially, i.e. one after the other?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 61

An IS auditor should use statistical sampling and not judgment (nonstatistical) sampling, when:

- ☐ the probability of error must be objectively quantified.
- ☐ the auditor wishes to avoid sampling risk.
- ☐ generalized audit software is unavailable.
- ☐ the tolerable error rate cannot be determined.

Question 62

In order to properly protect against unauthorized disclosure of sensitive data, how should hard disks be sanitized?

- ☐ The data should be deleted and overwritten with binary 0s.
- ☐ The data should be demagnetized.
- ☐ The data should be low-level formatted.
- ☐ The data should be deleted.

Question 63

An IS auditor issues an audit report pointing out the lack of firewall protection features at the perimeter network gateway and recommends a vendor product to address this vulnerability. The IS auditor has failed to exercise:

- ☐ professional independence
- ☐ organizational independence.
- ☐ technical competence.
- ☐ professional competence.

Question 64

What is an effective control for granting temporary access to vendors and external support personnel?

- ☐ Creating user accounts that automatically expire by a predetermined date
- ☐ Creating permanent guest accounts for temporary use
- ☐ Creating user accounts that restrict logon access to certain hours of the day
- ☐ Creating a single shared vendor administrator account on the basis of least-privileged access

Question 65

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?

- ☐ System owners
- ☐ System users
- ☐ System designers
- ☐ System builders

Question 66

Which of the following transmission media is MOST difficult to tap?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Radio System

Question 67

In determining the acceptable time period for the resumption of critical business processes:

- ☐ only downtime costs need to be considered.
- ☐ recovery operations should be analyzed.
- ☐ both downtime costs and recovery costs need to be evaluated.
- ☐ indirect downtime costs should be ignored.

Question 68

"Nowadays, computer security comprises mainly "preventive"" measures."

- ☐ True
- ☐ True only for trusted networks
- ☐ True only for untrusted networks
- ☐ False
- ☐ None of the choices.

Question 69

A critical function of a firewall is to act as a:

- ☐ special router that connects the Internet to a LAN.
- ☐ device for preventing authorized users from accessing the LAN.
- ☐ server used to connect authorized users to private trusted network resources.
- ☐ proxy server to increase the speed of access to authorized users.

Question 70

Which of the following is the unique identifier within an IPSec packet that enables the sending host to reference the security parameter to apply?

- ☐ SPI
- ☐ SA
- ☐ ESP
- ☐ AH

Question 71

Any changes in systems assets, such as replacement of hardware, should be immediately recorded within the assets inventory of which of the following?

- ☐ IT strategic plan
- ☐ Business continuity plan
- ☐ Business impact analysis
- ☐ Incident response plan

Question 72

Which of the following would effectively verify the originator of a transaction?

- ☐ Using a secret password between the originator and the receiver
- ☐ Encrypting the transaction with the receiver's public key
- ☐ Using a portable document format (PDF) to encapsulate transaction content
- ☐ Digitally signing the transaction with the source's private key

Question 73

Which of the following measures can protect systems files and data, respectively?

- ☐ User account access controls and cryptography
- ☐ User account access controls and firewall
- ☐ User account access controls and IPS
- ☐ IDS and cryptography
- ☐ Firewall and cryptography
- ☐ None of the choices.

Question 74

Which of the following satisfies a two-factor user authentication?

- ☐ Iris scanning plus fingerprint scanning
- ☐ Terminal ID plus global positioning system (GPS)
- ☐ A smart card requiring the user's PIN
- ☐ User ID along with password

Question 75

In the process of evaluating program change controls, an IS auditor would use source code comparison software to:

- ☐ examine source program changes without information from IS personnel.
- ☐ detect a source program change made between acquiring a copy of the source and the comparison run.
- ☐ confirm that the control copy is the current version of the production program.
- ☐ ensure that all changes made in the current source copy are detected.

Question 76

Which of the following sampling methods is MOST useful when testing for compliance?

- ☐ Attribute sampling
- ☐ Variable sampling
- ☐ Stratified mean per unit
- ☐ Difference estimation

Question 77

Who is responsible for implementing cost-effective controls in an automated system?

- ☐ Security policy administrators
- ☐ Business unit management
- ☐ Senior management
- ☐ Board of directors

Question 78

What type of BCP test uses actual resources to simulate a system crash and validate the plan's effectiveness?

- ☐ Paper
- ☐ Preparedness
- ☐ Walk-through
- ☐ Parallel

Question 79

Which of the following are effective in detecting fraud because they have the capability to consider a large number of variables when trying to resolve a problem?

- ☐ Expert systems
- ☐ Neural networks
- ☐ Integrated synchronized systems
- ☐ Multitasking applications

Question 80

Which of the following method is recommended by security professional to PERMANENTLY erase sensitive data on magnetic media?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Question 81

Identify the correct sequence of Business Process Reengineering (BPR) application steps from the given choices below?

- ☐ Envision, Initiate, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Initiate, Envision, Diagnose, Redesign, Reconstruct and Evaluate
- ☐ Envision, Diagnose, Initiate, Redesign, Reconstruct and Evaluate
- ☐ Evaluate, Envision, Initiate, Diagnose, Redesign, Reconstruct

Question 82

An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- ☐ Electromagnetic interference (EMI)
- ☐ Cross-talk
- ☐ Dispersion
- ☐ Attenuation

Question 83

Which of the following should an IS auditor review to understand project progress in terms of time, budget and deliverables for early detection of possible overruns and for projecting estimates at completion (EACs)?

- ☐ Function point analysis
- ☐ Earned value analysis
- ☐ Cost budget
- ☐ Program Evaluation and Review Technique

Question 84

An IS auditor reviewing the key roles and responsibilities of the database administrator (DBA) is LEAST likely to expect the job description of the DBA to include:

- ☐ defining the conceptual schema.
- ☐ defining security and integrity checks.
- ☐ liaising with users in developing data model.
- ☐ mapping data model with the internal schema.

Question 85

You may reduce a cracker's chances of success by (choose all that apply):

- ☐ keeping your systems up to date using a security scanner.
- ☐ hiring competent people responsible for security to scan and update your systems.
- ☐ using multiple firewalls.
- ☐ using multiple firewalls and IDS.
- ☐ None of the choices.

Question 86

An IS auditor reviews an organizational chart PRIMARILY for:

- ☐ an understanding of workflows.
- ☐ investigating various communication channels.
- ☐ understanding the responsibilities and authority of individuals.
- ☐ investigating the network connected to different employees.

Question 87

The PRIMARY objective of testing a business continuity plan is to:

- ☐ familiarize employees with the business continuity plan.
- ☐ ensure that all residual risks are addressed.
- ☐ exercise all possible disaster scenarios.
- ☐ identify limitations of the business continuity plan.

Question 88

While evaluating software development practices in an organization, an IS auditor notes that the quality assurance (QA) function reports to project management. The MOST important concern for an IS auditor is the:

- ☐ effectiveness of the QA function because it should interact between project management and user management
- ☐ efficiency of the QA function because it should interact with the project implementation team.
- ☐ effectiveness of the project manager because the project manager should interact with the QA function.
- ☐ efficiency of the project manager because the QA function will need to communicate with the project implementation team.

Question 89

Which of the following attack is also known as Time of Check(TOC)/Time of Use(TOU)?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Question 90

If an IS auditor observes that individual modules of a system perform correctly in development project tests, the auditor should inform management of the positive results and recommend further:

- ☐ Documentation development
- ☐ Comprehensive integration testing
- ☐ Full unit testing
- ☐ Full regression testing

Question 91

To determine who has been given permission to use a particular system resource, an IS auditor should review:

- ☐ activity lists.
- ☐ access control lists.
- ☐ logon ID lists.
- ☐ password lists.

Question 92

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as:

- ☐ wormnets
- ☐ trojannets
- ☐ spynets
- ☐ botnets
- ☐ rootnets
- ☐ backdoor

Question 93

During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:

- ☐ test data covering critical applications.
- ☐ detailed test plans.
- ☐ quality assurance test specifications.
- ☐ user acceptance testing specifications

Question 94

The use of a GANTT chart can:

- ☐ aid in scheduling project tasks.
- ☐ determine project checkpoints.
- ☐ ensure documentation standards.
- ☐ direct the post-implementation review.

Question 95

The MOST likely explanation for the use of applets in an Internet application is that:

- ☐ it is sent over the network from the server.
- ☐ the server does not run the program and the output is not sent over the network.
- ☐ they improve the performance of the web server and network.
- ☐ it is a JAVA program downloaded through the web browser and executed by the web server of the client machine.

Question 96

Which of the following is the INCORRECT "layer - protocol data unit (PDU)" mapping within the TCP/IP model?

- ☐ Application layer – Data
- ☐ Transport layer – Segment
- ☐ Network layer – Frame
- ☐ Physical layer – bits

Question 97

Who is mainly responsible for protecting information assets they have been entrusted with on a daily basis by defining who can access the data, its sensitivity level, type of access, and adhering to corporate information security policies?

- ☐ Data Owner
- ☐ Security Officer
- ☐ Senior Management
- ☐ End User

Question 98

When performing a computer forensic investigation, in regard to the evidence gathered, an IS auditor should be MOST concerned with:

- ☐ analysis.
- ☐ evaluation.
- ☐ preservation.
- ☐ disclosure.

Question 99

Which of the following types of attack makes use of common consumer devices that can be used to transfer data surreptitiously?

- ☐ Direct access attacks
- ☐ Indirect access attacks
- ☐ Port attack
- ☐ Window attack
- ☐ Social attack
- ☐ None of the choices.

Question 100

Which of the following should an IS auditor review to gain an understanding of the effectiveness of controls over the management of multiple projects?

- ☐ Project database
- ☐ Policy documents
- ☐ Project portfolio database
- ☐ Program organization

Question 101

Which of the following would provide the highest degree of server access control?

- ☐ A mantrap-monitored entryway to the server room
- ☐ Host-based intrusion detection combined with CCTV
- ☐ Network-based intrusion detection
- ☐ A fingerprint scanner facilitating biometric access control

Question 102

Which of the following is the process of feeding test data into two systems – the modified system and alternative system and comparing the result?

- ☐ Parallel Test
- ☐ Black box testing
- ☐ Regression Testing
- ☐ Pilot Testing

Question 103

Which of the following will replace system binaries and/or hook into the function calls of the operating system to hide the presence of other programs (choose the most precise answer)?

- ☐ rootkits
- ☐ virus
- ☐ trojan
- ☐ tripwire
- ☐ None of the choices.

Question 104

Which of the following programs would a sound information security policy MOST likely include to handle suspected intrusions?

- ☐ Response
- ☐ Correction
- ☐ Detection
- ☐ Monitoring

Question 105

Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?

- ☐ A sufficient quantity of data for each test case
- ☐ Data representing conditions that are expected in actual processing
- ☐ Completing the test on schedule
- ☐ A random sample of actual data

Question 106

Which of the following is a sophisticated computer based switch that can be thought of as essentially a small in-house phone company for the organization?

- ☐ Private Branch Exchange
- ☐ Virtual Local Area Network
- ☐ Voice over IP
- ☐ Dial-up connection

Question 107

Disabling which of the following would make wireless local area networks more secure against unauthorized access?

- ☐ MAC (Media Access Control) address filtering
- ☐ WPA (Wi-Fi Protected Access Protocol)
- ☐ LEAP (Lightweight Extensible Authentication Protocol)
- ☐ SSID (service set identifier) broadcasting

Question 108

During a review of a customer master file, an IS auditor discovered numerous customer name duplications arising from variations in customer first names. To determine the extent of the duplication, the IS auditor would use:

- ☐ test data to validate data input.
- ☐ test data to determine system sort capabilities.
- ☐ generalized audit software to search for address field duplications.
- ☐ generalized audit software to search for account field duplications.

Question 109

In an organization where an IT security baseline has been defined, an IS auditor should FIRST ensure:

- ☐ implementation.
- ☐ compliance.
- ☐ documentation.
- ☐ sufficiency.

Question 110

To optimize an organization's business contingency plan (BCP), an IS auditor should recommend conducting a business impact analysis (BIA) in order to determine:

- ☐ the business processes that generate the most financial value for the organization and therefore must be recovered first.
- ☐ the priorities and order for recovery to ensure alignment with the organization's business strategy.
- ☐ the business processes that must be recovered following a disaster to ensure the organization's survival.
- ☐ the priorities and order of recovery which will recover the greatest number of systems in the shortest time frame.

Question 111

Which of the following is a project management technique for defining and deploying software deliverables within a relatively short and fixed period of time, and with predetermined specific resources?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Critical path methodology
- ☐ Time box management

Question 112

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 113

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?

- ☐ Applications may not be subject to testing and IT general controls
- ☐ increased development and maintenance costs
- ☐ increased application development time
- ☐ Decision-making may be impaired due to diminished responsiveness to requests for information

Question 114

The MOST effective control for addressing the risk of piggybacking is:

- ☐ a single entry point with a receptionist.
- ☐ the use of smart cards.
- ☐ a biometric door lock.
- ☐ a deadman door.

Question 115

Which of the following system and data conversion strategies provides the GREATEST redundancy?

- ☐ Direct cutover
- ☐ Pilot study
- ☐ Phased approach
- ☐ Parallel run

Question 116

Which of the following statements pertaining to IPSec is incorrect?

- ☐ A security association has to be defined between two IPSec systems in order for bi-directional communication to be established.
- ☐ Integrity and authentication for IP datagrams are provided by AH.
- ☐ ESP provides for integrity, authentication and encryption to IP datagram's.
- ☐ In transport mode, ESP only encrypts the data payload of each packet.

Question 117

What must an IS auditor understand before performing an application audit?

- ☐ The potential business impact of application risks.
- ☐ Application risks must first be identified.
- ☐ Relative business processes.
- ☐ Relevant application risks.

Question 118

Which of the following is of greatest concern to the IS auditor?

- ☐ Failure to report a successful attack on the network
- ☐ Failure to prevent a successful attack on the network
- ☐ Failure to recover from a successful attack on the network
- ☐ Failure to detect a successful attack on the network

Question 119

When is regression testing used to determine whether new application changes have introduced any errors in the remaining unchanged code?

- ☐ In program development and change management
- ☐ In program feasibility studies
- ☐ In program development
- ☐ In change management

Question 120

An IS auditor attempting to determine whether access to program documentation is restricted to authorized persons would MOST likely:

- ☐ evaluate the record retention plans for off-premises storage.
- ☐ interview programmers about the procedures currently being followed.
- ☐ compare utilization records to operations schedules.
- ☐ review data file access records to test the librarian function.

Question 121

Codes from exploit programs are frequently reused in:

- ☐ trojan horses only.
- ☐ computer viruses only.
- ☐ OS patchers.
- ☐ eavedroppers.
- ☐ trojan horses and computer viruses.
- ☐ None of the choices.

Question 122

Which of the following attacks targets the Secure Sockets Layer (SSL)?

- ☐ Man-in-the middle
- ☐ Dictionary
- ☐ Password sniffing
- ☐ Phishing

Question 123

An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- ☐ compromises the Wireless Application Protocol (WAP) gateway.
- ☐ installs a sniffing program in front of the server.
- ☐ steals a customer's PDA.
- ☐ listens to the wireless transmission.

Question 124

Which of the following device in Frame Relay WAN technique is a service provider device that does the actual data transmission and switching in the frame relay cloud?

- ☐ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Question 125

Which of the following would be considered an essential feature of a network management system?

- ☐ A graphical interface to map the network topology
- ☐ Capacity to interact with the Internet to solve the problems
- ☐ Connectivity to a help desk for advice on difficult issues
- ☐ An export facility for piping data to spreadsheets

Question 126

A firm is considering using biometric fingerprint identification on all PCs that access critical data. This requires:

- ☐ that a registration process is executed for all accredited PC users.
- ☐ the full elimination of the risk of a false acceptance.
- ☐ the usage of the fingerprint reader be accessed by a separate password.
- ☐ assurance that it will be impossible to gain unauthorized access to critical data.

Question 127

Which of the following physical access controls effectively reduces the risk of piggybacking?

- ☐ Biometric door locks
- ☐ Combination door locks
- ☐ Deadman doors
- ☐ Bolting door locks

Question 128

Which of the following transmission media uses a transponder to send information?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 129

Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

- ☐ each plan is consistent with one another.
- ☐ all plans are integrated into a single plan.
- ☐ each plan is dependent on one another.
- ☐ the sequence for implementation of all plans is defined.

Question 130

Whenever an application is modified, what should be tested to determine the full impact of the change?

- ☐ Interface systems with other applications or systems
- ☐ The entire program, including any interface systems with other applications or systems
- ☐ All programs, including interface systems with other applications or systems
- ☐ Mission-critical functions and any interface systems with other applications or systems

Question 131

Who is primarily responsible for storing and safeguarding the data?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Steward
- ☐ Security Administrator

Question 132

Reverse proxy technology for web servers should be deployed if:

- ☐ http servers' addresses must be hidden.
- ☐ accelerated access to all published pages is required.
- ☐ caching is needed for fault tolerance.
- ☐ bandwidth to the user is limited.

Question 133

An IS auditor who was involved in designing an organization's business continuity plan (BCP) has been assigned to audit the plan. The IS auditor should:

- ☐ decline the assignment.
- ☐ inform management of the possible conflict of interest after completing the audit assignment.
- ☐ inform the business continuity planning (BCP) team of the possible conflict of interest prior to beginning the assignment.
- ☐ communicate the possibility of conflict of interest to management prior to starting the assignment.

Question 134

Digital signatures require the sender to "sign" the data by encrypting the data with the sender's public key, to then be decrypted by the recipient using the recipient's private key.

True or false?

- ☐ False
- ☐ True

Question 135

A live test of a mutual agreement for IT system recovery has been carried out, including a four-hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

- ☐ system and the IT operations team can sustain operations in the emergency environment.
- ☐ resources and the environment could sustain the transaction load.
- ☐ connectivity to the applications at the remote site meets response time requirements.
- ☐ workflow of actual business operations can use the emergency system in case of a disaster.

Question 136

What does PKI use to provide some of the strongest overall control over data confidentiality, reliability, and integrity for Internet transactions?

- ☐ A combination of public-key cryptography and digital certificates and two-factor authentication
- ☐ A combination of public-key cryptography and two-factor authentication
- ☐ A combination of public-key cryptography and digital certificates
- ☐ A combination of digital certificates and two-factor authentication

Question 137

While reviewing sensitive electronic work papers, the IS auditor noticed that they were not encrypted. This could compromise the:

- ☐ audit trail of the versioning of the work papers.
- ☐ approval of the audit phases.
- ☐ access rights to the work papers.
- ☐ confidentiality of the work papers.

Question 138

The role of the certificate authority (CA) as a third party is to:

- ☐ provide secured communication and networking services based on certificates.
- ☐ host a repository of certificates with the corresponding public and secret keys issued by that CA.
- ☐ act as a trusted intermediary between two communication partners.
- ☐ confirm the identity of the entity owning a certificate issued by that CA.

Question 139

Which of the following is a program evaluation review technique that considers different scenarios for planning and control projects?

- ☐ Function Point Analysis (FPA)
- ☐ GANTT
- ☐ Rapid Application Development (RAD)
- ☐ PERT

Question 140

The most likely error to occur when implementing a firewall is:

- ☐ incorrectly configuring the access lists.
- ☐ compromising the passwords due to social engineering.
- ☐ connecting a modem to the computers in the network.
- ☐ inadequately protecting the network and server from virus attacks.

Question 141

During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

- ☐ recommend that the BCP cover all business processes.
- ☐ assess the impact of the processes not covered.
- ☐ report the findings to the IT manager.
- ☐ redefine critical processes.

Question 142

Which of the following terms generally refers to small programs designed to take advantage of a software flaw that has been discovered?

- ☐ exploit
- ☐ patch
- ☐ quick fix
- ☐ service pack
- ☐ malware
- ☐ None of the choices.

Question 143

An IS auditor finds that not all employees are aware of the enterprise's information security policy. The IS auditor should conclude that:

- ☐ this lack of knowledge may lead to unintentional disclosure of sensitive information.
- ☐ information security is not critical to all functions.
- ☐ IS audit should provide security training to the employees.
- ☐ the audit finding will cause management to provide continuous training to staff.

Question 144

Regarding digital signature implementation, which of the following answers is correct?

- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
- ☐ A digital signature is created by the sender to prove message integrity by initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
- ☐ A digital signature is created by the sender to prove message integrity by encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Question 145

The PRIMARY purpose of audit trails is to:

- ☐ improve response time for users.
- ☐ establish accountability and responsibility for processed transactions.
- ☐ improve the operational efficiency of the system.
- ☐ provide useful information to auditors who may wish to track transactions

Question 146

A check digit is an effective edit check to:

- ☐ Detect data-transcription errors
- ☐ Detect data-transposition and transcription errors
- ☐ Detect data-transposition, transcription, and substitution errors
- ☐ Detect data-transposition errors

Question 147

An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?

- ☐ Simple Object Access Protocol (SOAP)
- ☐ Address Resolution Protocol (ARP)
- ☐ Routing Information Protocol (RIP)
- ☐ Transmission Control Protocol (TCP)

Question 148

A data administrator is responsible for:

- ☐ maintaining database system software.
- ☐ defining data elements, data names and their relationship.
- ☐ developing physical database structures.
- ☐ developing data dictionary system software.

Question 149

An IS auditor is assigned to audit a software development project which is more than 80 percent complete, but has already overrun time by 10 percent and costs by 25 percent. Which of the following actions should the IS auditor take?

- ☐ Report that the organization does not have effective project management.
- ☐ Recommend the project manager be changed.
- ☐ Review the IT governance structure.
- ☐ Review the conduct of the project and the business case.

Question 150

A malicious code that changes itself with each file it infects is called a:

- ☐ logic bomb.
- ☐ stealth virus.
- ☐ trojan horse.
- ☐ polymorphic virus.

Question 151

Which of the following BEST describes the concept of ""defense in depth""?

- ☐ more than one subsystem needs to be compromised to compromise the security of the system and the information it holds.
- ☐ multiple firewalls are implemented.
- ☐ multiple firewalls and multiple network OS are implemented.
- ☐ intrusion detection and firewall filtering are required.
- ☐ None of the choices.

Question 152

Which of the following is a distinctive feature of the Secure Electronic Transactions (SET) protocol when used for electronic credit card payments?

- ☐ The buyer is assured that neither the merchant nor any other party can misuse their credit card data.
- ☐ All personal SET certificates are stored securely in the buyer's computer.
- ☐ The buyer is liable for any transaction involving his/her personal SET certificates.
- ☐ The payment process is simplified, as the buyer is not required to enter a credit card number and an expiration date.

Question 153

In computer forensics, which of the following is the process that allows bit-for-bit copy of a data to avoid damage of original data or information when multiple analysis may be performed?

- ☐ Imaging
- ☐ Extraction
- ☐ Data Protection
- ☐ Data Acquisition

Question 154

Which of the following is an advantage of the top-down approach to software testing?

- ☐ Interface errors are identified early
- ☐ Testing can be started before all programs are complete
- ☐ it is more effective than other testing approaches
- ☐ Errors in critical modules are detected sooner

Question 155

The PRIMARY objective of business continuity and disaster recovery plans should be to:

- ☐ safeguard critical IS assets.
- ☐ provide for continuity of operations.
- ☐ minimize the loss to an organization.
- ☐ protect human life.

Question 156

Which of the following attack includes social engineering, link manipulation or web site forgery techniques?

- ☐ surf attack
- ☐ Traffic analysis
- ☐ Phishing
- ☐ Interrupt attack

Question 157

Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?

- ☐ A hot site contracted and available as needed.
- ☐ A business continuity manual is available and current.
- ☐ insurance coverage is adequate and premiums are current.
- ☐ Media backups are performed on a timely basis and stored offsite.

Question 158

IT control objectives are useful to IS auditors, as they provide the basis for understanding the:

- ☐ desired result or purpose of implementing specific control procedures.
- ☐ best IT security control practices relevant to a specific entity.
- ☐ techniques for securing information.
- ☐ security policy.

Question 159

Which of the following term related to network performance refers to the delay that packet may experience on their way to reach the destination from the source?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 160

When assessing the design of network monitoring controls, an IS auditor should FIRST review network:

- ☐ topology diagrams.
- ☐ bandwidth usage.
- ☐ traffic analysis reports.
- ☐ bottleneck locations.

Question 161

Which of the following level in CMMI model focuses on process definition and process deployment?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Question 162

Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

- ☐ Simple Network Management Protocol
- ☐ File Transfer Protocol
- ☐ Simple Mail Transfer Protocol
- ☐ Telnet

Question 163

Which of the following is NOT a component of IPSec?

- ☐ Authentication Header
- ☐ Encapsulating Security Payload
- ☐ Key Distribution Center
- ☐ Internet Key Exchange

Question 164

The IS management of a multinational company is considering upgrading its existing virtual private network (VPN) to support voice-over IP (VoIP) communications via tunneling. Which of the following considerations should be PRIMARILY addressed?

- ☐ Reliability and quality of service (QoS)
- ☐ Means of authentication
- ☐ Privacy of voice transmissions
- ☐ Confidentiality of data transmissions

Question 165

Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?

- ☐ Intrusion detection systems
- ☐ Data mining techniques
- ☐ Firewalls
- ☐ Packet filtering routers

Question 166

Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?

- ☐ Overwriting the tapes
- ☐ initializing the tape labels
- ☐ Degaussing the tapes
- ☐ Erasing the tapes

Question 167

What type of cryptosystem is characterized by data being encrypted by the sender using the recipient's public key, and the data then being decrypted using the recipient's private key?

- ☐ With public-key encryption, or symmetric encryption
- ☐ With public-key encryption, or asymmetric encryption
- ☐ With shared-key encryption, or symmetric encryption
- ☐ With shared-key encryption, or asymmetric encryption

Question 168

Which of the following is a passive attack method used by intruders to determine potential network vulnerabilities?

- ☐ Traffic analysis
- ☐ SYN flood
- ☐ Denial of service (DoS)
- ☐ Distributed denial of service (DoS)

Question 169

What can be implemented to provide the highest level of protection from external attack?

- ☐ Layering perimeter network protection by configuring the firewall as a screened host in a screened subnet behind the bastion host
- ☐ Configuring the firewall as a screened host behind a router
- ☐ Configuring the firewall as the protecting bastion host
- ☐ Configuring two load-sharing firewalls facilitating VPN access from external hosts to internal hosts

Question 170

Effective IT governance requires organizational structures and processes to ensure that:

- ☐ the organization's strategies and objectives extend the IT strategy.
- ☐ the business strategy is derived from an IT strategy.
- ☐ IT governance is separate and distinct from the overall governance.
- ☐ the IT strategy extends the organization's strategies and objectives.

Question 171

Which of the following is an advantage of an integrated test facility (ITF)?

- ☐ It uses actual master files or dummies and the IS auditor does not have to review the source of the transaction.
- ☐ Periodic testing does not require separate test processes.
- ☐ It validates application systems and tests the ongoing operation of the system.
- ☐ The need to prepare test data is eliminated.

Question 172

An IS auditor invited to a development project meeting notes that no project risks have been documented. When the IS auditor raises this issue, the project manager responds that it is too early to identify risks and that, if risks do start impacting the project, a risk manager will be hired. The appropriate response of the IS auditor would be to:

- ☐ stress the importance of spending time at this point in the project to consider and document risks, and to develop contingency plans.
- ☐ accept the project manager's position as the project manager is accountable for the outcome of the project.
- ☐ offer to work with the risk manager when one is appointed.
- ☐ inform the project manager that the IS auditor will conduct a review of the risks at the completion of the requirements definition phase of the project.

Question 173

The MOST likely explanation for a successful social engineering attack is:

- ☐ that computers make logic errors.
- ☐ that people make judgment errors.
- ☐ the computer knowledge of the attackers.
- ☐ the technological sophistication of the attack method.

Question 174

Which of the following attack could be avoided by creating more security awareness in the organization and provide adequate security knowledge to all employees?

- ☐ surf attack
- ☐ Traffic analysis
- ☐ Phishing
- ☐ Interrupt attack

Question 175

The 'trusted systems' approach has been predominant in the design of:

- ☐ many earlier Microsoft OS products
- ☐ the IBM AS/400 series
- ☐ the SUN Solaris series
- ☐ most OS products in the market
- ☐ None of the choices.

Question 176

To affix a digital signature to a message, the sender must first create a message digest by applying a cryptographic hashing algorithm against:

- ☐ the entire message and thereafter enciphering the message digest using the sender's private key.
- ☐ any arbitrary part of the message and thereafter enciphering the message digest using the sender's private key.
- ☐ the entire message and thereafter enciphering the message using the sender's private key.
- ☐ the entire message and thereafter enciphering the message along with the message digest using the sender's private key.

Question 177

Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?

- ☐ A program that deposits a virus on a client machine
- ☐ Applets recording keystrokes and, therefore, passwords
- ☐ Downloaded code that reads files on a client's hard drive
- ☐ Applets opening connections from the client machine

Question 178

IS management recently replaced its existing wired local area network (LAN) with a wireless infrastructure to accommodate the increased use of mobile devices within the organization. This will increase the risk of which of the following attacks?

- ☐ Port scanning
- ☐ Back door
- ☐ Man-in-the-middle
- ☐ War driving

Question 179

Which of the following cryptographic systems is MOST appropriate for bulk data encryption and small devices such as smart cards?

- ☐ DES
- ☐ AES
- ☐ Triple DES
- ☐ RSA

Question 180

Which of the following ensures a sender's authenticity and an e-mail's confidentiality?

- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the hash of the message with the receiver's public key
- ☐ The sender digitally signing the message and thereafter encrypting the hash of the message with the sender's private key
- ☐ Encrypting the hash of the message with the sender's private key and thereafter encrypting the message with the receiver's public key
- ☐ Encrypting the message with the sender's private key and encrypting the message hash with the receiver's public key.

Question 181

Which of the following hardware devices relieves the central computer from performing network control, format conversion and message handling tasks?

- ☐ Spool
- ☐ Cluster controller
- ☐ Protocol converter
- ☐ Front end processor

Question 182

When reviewing an organization's strategic IT plan an IS auditor should expect to find:

- ☐ an assessment of the fit of the organization's application portfolio with business objectives.
- ☐ actions to reduce hardware procurement cost.
- ☐ a listing of approved suppliers of IT contract resources.
- ☐ a description of the technical architecture for the organization's network perimeter security.

Question 183

Which of the following layer in an enterprise data flow architecture derives enterprise information from operational data, external data and nonoperational data?

- ☐ Data preparation layer
- ☐ Data source layer
- ☐ Data mart layer
- ☐ Data access layer

Question 184

An IS auditor reviewing access controls for a client-server environment should FIRST:

- ☐ evaluate the encryption technique.
- ☐ identify the network access points.
- ☐ review the identity management system.
- ☐ review the application level access controls.

Question 185

Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

- ☐ translating and unbundling transactions.
- ☐ routing verification procedures.
- ☐ passing data to the appropriate application system.
- ☐ creating a point of receipt audit log.

Question 186

Which of the following attack is MOSTLY performed by an attacker to steal the identity information of a user such as credit card number, passwords, etc?

- ☐ Smurf attack
- ☐ Traffic analysis
- ☐ Harming
- ☐ Interrupt attack

Question 187

Proper segregation of duties does not prohibit a quality control administrator from also being responsible for change control and problem management. True or false?

- ☐ True
- ☐ False

Question 188

When reviewing an active project, an IS auditor observed that, because of a reduction in anticipated benefits and increased costs, the business case was no longer valid. The IS auditor should recommend that the:

- ☐ project be discontinued.
- ☐ business case be updated and possible corrective actions be identified.
- ☐ project be returned to the project sponsor for reapproval.
- ☐ project be completed and the business case be updated later.

Question 189

Proper segregation of duties prevents a computer operator (user) from performing security administration duties. True or false?

- ☐ True
- ☐ False

Question 190

A call-back system requires that a user with an id and password call a remote server through a dial-up line, then the server disconnects and:

- ☐ dials back to the user machine based on the user id and password using a telephone number from its database.
- ☐ dials back to the user machine based on the user id and password using a telephone number provided by the user during this connection.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using its database.
- ☐ waits for a redial back from the user machine for reconfirmation and then verifies the user id and password using the sender's database.

Question 191

While planning an audit, an assessment of risk should be made to provide:

- ☐ reasonable assurance that the audit will cover material items.
- ☐ definite assurance that material items will be covered during the audit work.
- ☐ reasonable assurance that all items will be covered by the audit.
- ☐ sufficient assurance that all items will be covered during the audit work.

Question 192

As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?

- ☐ Organizational risks, such as single point-of-failure and infrastructure risk
- ☐ Threats to critical business processes
- ☐ Critical business processes for ascertaining the priority for recovery
- ☐ Resources required for resumption of business

Question 193

Which of the following term describes a failure of an electric utility company to supply power within acceptable range?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☐ EMI

Question 194

Which of the following should an IS auditor recommend to BEST enforce alignment of an IT project portfolio with strategic organizational priorities?

- ☐ Define a balanced scorecard (BSC) for measuring performance
- ☐ Consider user satisfaction in the key performance indicators (KPIs)
- ☐ Select projects according to business benefits and risks
- ☐ Modify the yearly process of defining the project portfolio

Question 195

The final decision to include a material finding in an audit report should be made by the:

- ☐ audit committee.
- ☐ auditee's manager.
- ☐ IS auditor.
- ☐ CEO of the organization

Question 196

What can be used to help identify and investigate unauthorized transactions?

- ☐ Postmortem review
- ☐ Reasonableness checks
- ☐ Data-mining techniques
- ☐ Expert systems

Question 197

An integrated test facility is considered a useful audit tool because it:

- ☐ is a cost-efficient approach to auditing application controls.
- ☐ enables the financial and IS auditors to integrate their audit tests.
- ☐ compares processing output with independently calculated data.
- ☐ provides the IS auditor with a tool to analyze a large range of information

Question 198

An IS auditor is performing an audit of a network operating system. Which of the following is a user feature the IS auditor should review?

- ☐ Availability of online network documentation
- ☐ Support of terminal access to remote hosts
- ☐ Handling file transfer between hosts and interuser communications
- ☐ Performance management, audit and control

Question 199

At the completion of a system development project, a post project review should include which of the following?

- ☐ Assessing risks that may lead to downtime after the production release
- ☐ Identifying lessons learned that may be applicable to future projects
- ☐ Verifying the controls in the delivered system are working
- ☐ Ensuring that test data are deleted

Question 200

In an IS audit of several critical servers, the IS auditor wants to analyze audit trails to discover potential anomalies in user or system behavior. Which of the following tools are MOST suitable for performing that task?

- ☐ CASE tools
- ☐ Embedded data collection tools
- ☐ Heuristic scanning tools
- ☐ Trend/variance detection tools

Question 201

Which of the following is protocol data unit (PDU) of data at LAN or WAN interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame and bits

Question 202

To protect a VoIP infrastructure against a denial-of-service (DoS) attack, it is MOST important to secure the:

- ☐ access control servers.
- ☐ session border controllers.
- ☐ backbone gateways.
- ☐ intrusion detection system (IDS).

Question 203

An advantage in using a bottom-up vs. a top-down approach to software testing is that:

- ☐ interface errors are detected earlier.
- ☐ confidence in the system is achieved earlier.
- ☐ errors in critical modules are detected earlier.
- ☐ major functions and processing are tested earlier.

Question 204

In a public key infrastructure, a registration authority:

- ☐ verifies information supplied by the subject requesting a certificate.
- ☐ issues the certificate after the required attributes are verified and the keys are generated.
- ☐ digitally signs a message to achieve nonrepudiation of the signed message.
- ☐ registers signed messages to protect them from future repudiation.

Question 205

When evaluating the collective effect of preventive, detective or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☐ The point at which controls are exercised as data flow through the system
- ☐ Only preventive and detective controls are relevant
- ☐ Corrective controls can only be regarded as compensating
- ☐ Classification allows an IS auditor to determine which controls are missing

Question 206

Which of the following term related to network performance refers to the actual rate that information is transferred over a network?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 207

To prevent IP spoofing attacks, a firewall should be configured to drop a packet if:

- ☐ the source routing field is enabled.
- ☐ it has a broadcast address in the destination field.
- ☐ a reset flag (RST) is turned on for the TCP connection.
- ☐ dynamic routing is used instead of static routing.

Question 208

What are used as the framework for developing logical access controls?

- ☐ Information systems security policies
- ☐ Organizational security policies
- ☐ Access Control Lists (ACL)
- ☐ Organizational charts for identifying roles and responsibilities

Question 209

Which of the following is an attribute of the control self-assessment (CSA) approach?

- ☐ Broad stakeholder involvement
- ☐ Auditors are the primary control analysts
- ☐ Limited employee participation
- ☐ Policy driven

Question 210

Why does an IS auditor review an organization chart?

- ☐ To optimize the responsibilities and authority of individuals
- ☐ To control the responsibilities and authority of individuals
- ☐ To better understand the responsibilities and authority of individuals
- ☐ To identify project sponsors

Question 211

Which of the following is the BEST way to satisfy a two-factor user authentication?

- ☐ A smart card requiring the user's PIN
- ☐ User ID along with password
- ☐ Iris scanning plus fingerprint scanning
- ☐ A magnetic card requiring the user's PIN

Question 212

Which of the following is the MOST important element for the successful implementation of IT governance?

- ☐ Implementing an IT scorecard
- ☐ Identifying organizational strategies
- ☐ Performing a risk assessment
- ☐ Creating a formal security policy

Question 213

When auditing third-party service providers, an IS auditor should be concerned with which of the following?

- ☐ Ownership of the programs and files
- ☐ A statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster
- ☐ A statement of due care
- ☐ Ownership of programs and files, a statement of due care and confidentiality, and the capability for continued service of the service provider in the event of a disaster

Question 214

Which of the following audit techniques would BEST aid an auditor in determining whether there have been unauthorized program changes since the last authorized program update?

- ☐ Test data run
- ☐ Code review
- ☐ Automated code comparison
- ☐ Review of code migration procedures

Question 215

An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

- ☐ alignment of the BCP with industry best practices.
- ☐ results of business continuity tests performed by IS and end-user personnel.
- ☐ off-site facility, its contents, security and environmental controls.
- ☐ annual financial cost of the BCP activities versus the expected benefit of implementation of the plan.

Question 216

At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:

- ☐ report the error as a finding and leave further exploration to the auditee's discretion.
- ☐ attempt to resolve the error.
- ☐ recommend that problem resolution be escalated.
- ☐ ignore the error, as it is not possible to get objective evidence for the software error.

Question 217

The BEST method of proving the accuracy of a system tax calculation is by:

- ☐ detailed visual review and analysis of the source code of the calculation programs
- ☐ recreating program logic using generalized audit software to calculate monthly totals.
- ☐ preparing simulated transactions for processing and comparing the results to predetermined results.
- ☐ automatic flowcharting and analysis of the source code of the calculation programs.

Question 218

While implementing an invoice system, Lily has implemented a database control which checks that new transactions are matched to those previously input to ensure that they have not already been entered. Which of the following control is implemented by Lily?

- ☐ Range Check
- ☐ Duplicate Check
- ☐ Existence check
- ☐ Reasonableness check

Question 219

Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?

- ☐ verify compatibility with the hot site.
- ☐ Review the implementation report.
- ☐ Perform a walk-through of the disaster recovery plan.
- ☐ Update the IS assets inventory.

Question 220

"Under the concept of ""defense in depth"", subsystems should be designed to:"

- ☐ ""fail insecure""
- ☐ ""fail secure""
- ☐ ""react to attack""
- ☐ ""react to failure""
- ☐ None of the choices.

Question 221

What is a primary high-level goal for an auditor who is reviewing a system development project?

- ☐ To ensure that programming and processing environments are segregated
- ☐ To ensure that proper approval for the project has been obtained
- ☐ To ensure that business objectives are achieved
- ☐ To ensure that projects are monitored and administrated effectively

Question 222

The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- ☐ Replay
- ☐ Brute force
- ☐ Cryptographic
- ☐ Mimic

Question 223

The PRIMARY purpose of an IT forensic audit is:

- ☐ to participate in investigations related to corporate fraud.
- ☐ the systematic collection of evidence after a system irregularity.
- ☐ to assess the correctness of an organization's financial statements
- ☐ to determine that there has been criminal activity.

Question 224

The use of object-oriented design and development techniques would MOST likely:

- ☐ facilitate the ability to reuse modules.
- ☐ improve system performance.
- ☐ enhance control effectiveness.
- ☐ speed up the system development life cycle.

Question 225

Which of the following statement INCORRECTLY describes Asynchronous Transfer Mode (ATM) technique?

- ☐ ATM uses cell switching method
- ☐ ATM is high speed network technology used for LAN, MAN and WAN
- ☐ ATM works at session layer of an OSI model
- ☐ Data are segmented into fixed size cell of 53 bytes

Question 226

Which of the following intrusion detection systems (IDSs) will MOST likely generate false alarms resulting from normal network activity?

- ☐ Statistical-based
- ☐ Signature-based
- ☐ Neural network
- ☐ Host-based

Question 227

Which of the following term related to network performance refers to the number of corrupted bits expressed as a percentage or fraction of the total sent?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Error Rate

Question 228

What supports data transmission through split cable facilities or duplicate cable facilities?

- ☐ Diverse routing
- ☐ Dual routing
- ☐ Alternate routing
- ☐ Redundant routing

Question 229

An organization is implementing an enterprise resource planning (ERP) application to meet its business objectives. Of the following, who is PRIMARILY responsible for overseeing the project in order to ensure that it is progressing in accordance with the project plan and that it will deliver the expected results?

- ☐ Project sponsor
- ☐ System development project team (SPDT)
- ☐ Project steering committee
- ☐ User project team (UPT)

Question 230

Which of the following software tools is often used for stealing money from infected PC owner through taking control of the modem?

- ☐ System patcher
- ☐ Porn dialer
- ☐ War dialer
- ☐ T1 dialer
- ☐ T3 dialer
- ☐ None of the choices.

Question 231

If an IS auditor finds evidence of risk involved in not implementing proper segregation of duties, such as having the security administrator perform an operations function, what is the auditor's primary responsibility?

- ☐ To advise senior management.
- ☐ To reassign job functions to eliminate potential fraud.
- ☐ To implement compensator controls.
- ☐ Segregation of duties is an administrative control not considered by an IS auditor.

Question 232

An IS auditor interviewing a payroll clerk finds that the answers do not support job descriptions and documented procedures. Under these circumstances, the IS auditor should:

- ☐ conclude that the controls are inadequate.
- ☐ expand the scope to include substantive testing
- ☐ place greater reliance on previous audits.
- ☐ suspend the audit.

Question 233

An IT steering committee should review information systems PRIMARILY to assess:

- ☐ whether IT processes support business requirements.
- ☐ if proposed system functionality is adequate
- ☐ the stability of existing software.
- ☐ the complexity of installed technology.

Question 234

When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:

- ☐ an integrated services digital network (ISDN) data link.
- ☐ traffic engineering.
- ☐ wired equivalent privacy (WEP) encryption of data.
- ☐ analog phone terminals.

Question 235

During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:

- ☐ an unauthorized user may use the ID to gain access.
- ☐ user access management is time consuming.
- ☐ passwords are easily guessed.
- ☐ user accountability may not be established.

Question 236

Which of the following types of transmission media provide the BEST security against unauthorized access?

- ☐ Copper wire
- ☐ Twisted pair
- ☐ Fiberoptic cables
- ☐ Coaxial cables

Question 237

What method might an IS auditor utilize to test wireless security at branch office locations?

- ☐ War dialing
- ☐ Social engineering
- ☐ War driving
- ☐ Password cracking

Question 238

Which of the following statement correctly describes the difference between total flooding and local application extinguishing agent?

- ☐ The local application design contain physical barrier enclosing the fire space where as physical barrier is not present in total flooding extinguisher
- ☐ The total flooding design contain physical barrier enclosing the fire space where as physical barrier is not present in local application design extinguisher
- ☐ The physical barrier enclosing fire space is not present in total flooding and local application extinguisher agent
- ☐ The physical barrier enclosing fire space is present in total flooding and local application extinguisher agent

Question 239

The MAIN criterion for determining the severity level of a service disruption incident is:

- ☐ cost of recovery.
- ☐ negative public opinion.
- ☐ geographic location.
- ☐ downtime.

Question 240

Of the three major types of off-site processing facilities, what type is characterized by at least providing for electricity and HVAC?

- ☐ Cold site
- ☐ Alternate site
- ☐ Hot site
- ☐ Warm site

Question 241

Most access violations are:

- ☐ Accidental
- ☐ Caused by internal hackers
- ☐ Caused by external hackers
- ☐ Related to Internet

Question 242

Which of the following Confidentiality, Integrity, Availability (CIA) attribute supports the principle of least privilege by providing access to information only to authorized and intended users?

- ☐ Confidentiality
- ☐ Integrity
- ☐ Availability
- ☐ Accuracy

Question 243

What are often the primary safeguards for systems software and data?

- ☐ Administrative access controls
- ☐ Logical access controls
- ☐ Physical access controls
- ☐ Detective access controls

Question 244

Which of the following INCORRECTLY describes the layer functions of the LAN or WAN Layer of the TCP/IP model?

- ☐ Combines packets into bytes and bytes into frame
- ☐ Provides logical addressing which routers use for path determination
- ☐ Provide address to media using MAC address
- ☐ Performs only error detection

Question 245

The FIRST step in managing the risk of a cyber-attack is to:

- ☐ assess the vulnerability impact.
- ☐ evaluate the likelihood of threats.
- ☐ identify critical information assets.
- ☐ estimate potential damage.

Question 246

Allowing application programmers to directly patch or change code in production programs increases risk of fraud. True or false?

- ☐ True
- ☐ False

Question 247

Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- ☐ Financial impact per security incident
- ☐ Number of security vulnerabilities that were patched
- ☐ Percentage of business applications that are being protected
- ☐ Number of successful penetration tests

Question 248

Which of the following fire suppression systems is MOST appropriate to use in a data center environment?

- ☐ Wet-pipe sprinkler system
- ☐ Dry-pipe sprinkler system
- ☐ FM-200system
- ☐ Carbon dioxide-based fire extinguishers

Question 249

When developing a security architecture, which of the following steps should be executed FIRST?

- ☐ Developing security procedures
- ☐ Defining a security policy
- ☐ Specifying an access control methodology
- ☐ Defining roles and responsibilities

Question 250

Which of the following provides the best evidence of the adequacy of a security awareness program?

- ☐ The number of stakeholders including employees trained at various levels
- ☐ Coverage of training at all locations across the enterprise
- ☐ The implementation of security devices from different vendors
- ☐ Periodic reviews and comparison with best practices

Question 251

Which of the following statement correctly describes difference between SSL and S/HTTP?

- ☐ Both works at application layer of OSI model
- ☐ SSL works at transport layer where as S/HTTP works at application layer of OSI model
- ☐ Both works at transport layer
- ☐ S/HTTP works at transport layer where as SSL works at the application layer of OSI model

Question 252

An accuracy measure for a biometric system is:

- ☐ system response time.
- ☐ registration time.
- ☐ input file size.
- ☐ false-acceptance rate.

Question 253

Which of the following type of computer is a large, general purpose computer that are made to share their processing power and facilities with thousands of internal or external users?

- ☐ Thin client computer
- ☐ Midrange servers
- ☐ Personal computers
- ☐ Mainframe computers

Question 254

A hub is a device that connects:

- ☐ two LANs using different protocols.
- ☐ a LAN with a WAN.
- ☐ a LAN with a metropolitan area network (MAN).
- ☐ two segments of a single LAN.

Question 255

Parity bits are a control used to validate:

- ☐ Data authentication
- ☐ Data completeness
- ☐ Data source
- ☐ Data accuracy

Question 256

Which of the following functionality is NOT performed by the application layer of a TCP/IP model?

- ☐ Print service, application services
- ☐ Data encryption and compression
- ☐ Dialog management
- ☐ End-to-end connection

Question 257

Which of the following protocol does NOT work at Network interface layer in TCP/IP model?

- ☐ ICMP
- ☐ DNS
- ☐ ARP
- ☐ Internet protocol

Question 258

Identify the INCORRECT statement from below mentioned testing types

- ☐ Recovery Testing – Making sure the modified/new system includes provisions for appropriate access control and does not introduce any security holes that might compromise other systems
- ☐ Load Testing – Testing an application with large quantities of data to evaluate its performance during peak hour
- ☐ Volume testing – Studying the impact on the application by testing with an incremental volume of records to determine the maximum volume of records that application can process
- ☐ Stress Testing – Studying the impact on the application by testing with an incremental number of concurrent users/services on the application to determine maximum number of concurrent user/service the application can process

Question 259

Which of the following would MOST likely indicate that a customer data warehouse should remain in-house rather than be outsourced to an offshore operation?

- ☐ Time zone differences could impede communications between IT teams.
- ☐ Telecommunications cost could be much higher in the first year.
- ☐ Privacy laws could prevent cross-border flow of information.
- ☐ Software development may require more detailed specifications.

Question 260

During an IS audit, auditor has observed that authentication and authorization steps are split into two functions and there is a possibility to force the authorization step to be completed before the authentication step. Which of the following technique an attacker could use to force authorization step before authentication?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Race Condition

Question 261

During an IS audit, one of your auditor has observed that some of the critical servers in your organization can be accessed ONLY by using shared/common user name and password. What should be the auditor's PRIMARY concern be with this approach?

- ☐ Password sharing
- ☐ Accountability
- ☐ Shared account management
- ☐ Difficulty in auditing shared account

Question 262

When storing data archives off-site, what must be done with the data to ensure data completeness?

- ☐ The data must be normalized.
- ☐ The data must be validated.
- ☐ The data must be parallel-tested.
- ☐ The data must be synchronized.

Question 263

During the review of a biometrics system operation, an IS auditor should FIRST review the stage of:

- ☐ enrollment.
- ☐ identification.
- ☐ verification.
- ☐ storage.

Question 264

Private Branch Exchange(PBX) environment involves many security risks, one of which is the people both internal and external to an organization. Which of the following risks are NOT associated with Private Branch Exchange?

1. Theft of service
2. Disclosure of information
3. Data Modifications
4. Denial of service
5. Traffic Analysis

- ☐ 3 and 4
- ☐ 4 and 5
- ☐ 1-4
- ☐ They are ALL risks associated with PBX

Question 265

An IS auditor's PRIMARY concern when application developers wish to use a copy of yesterday's production transaction file for volume tests is that:

- ☐ users may prefer to use contrived data for testing.
- ☐ unauthorized access to sensitive data may result.
- ☐ error handling and credibility checks may not be fully proven.
- ☐ the full functionality of the new process may not necessarily be tested.

Question 266

Attack amplifier is often being HEAVILY relied upon on by which of the following types of attack?

- ☐ Packet dropping
- ☐ ToS
- ☐ DDoS
- ☐ ATP
- ☐ Wiretapping
- ☐ None of the choices.

Question 267

Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits vulnerability in a protocol?

- ☐ Install the vendor's security fix for the vulnerability.
- ☐ Block the protocol traffic in the perimeter firewall.
- ☐ Block the protocol traffic between internal network segments.
- ☐ Stop the service until an appropriate security fix is installed.

Question 268

What is a common vulnerability, allowing denial-of-service attacks?

- ☐ Assigning access to users according to the principle of least privilege
- ☐ Lack of employee awareness of organizational security policies
- ☐ Improperly configured routers and router access lists
- ☐ Configuring firewall access rules

Question 269

In an audit of an inventory application, which approach would provide the BEST evidence that purchase orders are valid?

- ☐ Testing whether inappropriate personnel can change application parameters
- ☐ Tracing purchase orders to a computer listing
- ☐ Comparing receiving reports to purchase order details
- ☐ Reviewing the application documentation

Question 270

After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?

- ☐ Test and maintain the plan.
- ☐ Develop a specific plan.
- ☐ Develop recovery strategies.
- ☐ implement the plan.

Question 271

An IS auditor has been asked to participate in project initiation meetings for a critical project. The IS auditor's MAIN concern should be that the:

- ☐ complexity and risks associated with the project have been analyzed.
- ☐ resources needed throughout the project have been determined.
- ☐ project deliverables have been identified.
- ☐ a contract for external parties involved in the project has been completed.

Question 272

Which of the following layer of an enterprise data flow architecture is concerned with the assembly and preparation of data for loading into data marts?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 273

An IS auditor should aware of various analysis models used by data architecture. Which of the following analysis model outline the major process of an organization and the external parties with which business interacts?

- ☐ Context Diagrams
- ☐ Activity Diagrams
- ☐ Swim-lane diagrams
- ☐ Entity relationship diagrams

Question 274

Effective IT governance will ensure that the IT plan is consistent with the organization's:

- ☐ business plan.
- ☐ audit plan.
- ☐ security plan.
- ☐ investment plan.

Question 275

Which of the following is a benefit of a risk-based approach to audit planning? Audit:

- ☐ scheduling may be performed months in advance.
- ☐ budgets are more likely to be met by the IS audit staff.
- ☐ staff will be exposed to a variety of technologies.
- ☐ resources are allocated to the areas of highest concern

Question 276

During the collection of forensic evidence, which of the following actions would MOST likely result in the destruction or corruption of evidence on a compromised system?

- ☐ Dumping the memory content to a file
- ☐ Generating disk images of the compromised system
- ☐ Rebooting the system
- ☐ Removing the system from the network

Question 277

Corrective action has been taken by an auditee immediately after the identification of a reportable finding. The auditor should:

- ☐ include the finding in the final report, because the IS auditor is responsible for an accurate report of all findings.
- ☐ not include the finding in the final report, because the audit report should include only unresolved findings.
- ☐ not include the finding in the final report, because corrective action can be verified by the IS auditor during the audit.
- ☐ include the finding in the closing meeting for discussion purposes only.

Question 278

The specific advantage of white box testing is that it:

- ☐ verifies a program can operate successfully with other parts of the system.
- ☐ ensures a program's functional operating effectiveness without regard to the internal program structure.
- ☐ determines procedural accuracy or conditions of a program's specific logic paths.
- ☐ examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system.

Question 279

During the system testing phase of an application development project the IS auditor should review the:

- ☐ conceptual design specifications.
- ☐ vendor contract.
- ☐ error reports.
- ☐ program change requests.

Question 280

Which of the following fire-suppression methods is considered to be the most environmentally friendly?

- ☐ Halon gas
- ☐ Deluge sprinklers
- ☐ Dry-pipe sprinklers
- ☐ Wet-pipe sprinklers

Question 281

The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:

- ☐ facilitates user involvement.
- ☐ allows early testing of technical features.
- ☐ facilitates conversion to the new system.
- ☐ shortens the development time frame.

Question 282

Which of the following protocol does NOT work at the Application layer of the TCP/IP Models?

- ☐ HTTP
- ☐ FTP
- ☐ NTP
- ☐ TCP

Question 283

Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?

- ☐ Session keys are dynamic
- ☐ Private symmetric keys are used
- ☐ Keys are static and shared
- ☐ Source addresses are not encrypted or authenticated

Question 284

Which of the following option INCORRECTLY describes PBX feature?

- ☐ Voice mail -Stores messages centrally and – by using a password – allows for retrieval from inside or outside lines.
- ☐ Tenanting-Provides for the possibility to break into a busy line to inform another user an important message
- ☐ Automatic Call Distribution - Allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available
- ☐ Diagnostics -Allows for bypassing normal call restriction procedures

Question 285

An IS auditor has imported data from the client's database. The next step-confirming whether the imported data are complete-is performed by:

- ☐ matching control totals of the imported data to control totals of the original data.
- ☐ sorting the data to confirm whether the data are in the same order as the original data.
- ☐ reviewing the printout of the first 100 records of original data with the first 100 records of imported data.
- ☐ filtering data for different categories and matching them to the original data.

Question 286

When using a digital signature, the message digest is computed:

- ☐ only by the sender.
- ☐ only by the receiver.
- ☐ by both the sender and the receiver.
- ☐ by the certificate authority (CA).

Question 287

Establishing data ownership is an important first step for which of the following processes?

- ☐ Assigning user access privileges
- ☐ Developing organizational security policies
- ☐ Creating roles and responsibilities
- ☐ Classifying data

Question 288

Sending a message and a message hash encrypted by the sender's private key will ensure:

- ☐ authenticity and integrity.
- ☐ authenticity and privacy.
- ☐ integrity and privacy.
- ☐ privacy and nonrepudiation.

Question 289

In auditing a web server, an IS auditor should be concerned about the risk of individuals gaining unauthorized access to confidential information through:

- ☐ common gateway interface (CGI) scripts.
- ☐ enterprise Java beans (EJBs).
- ☐ applets.
- ☐ web services.

Question 290

What type(s) of firewalls provide(s) the greatest degree of protection and control because both firewall technologies inspect all seven OSI layers of network traffic?

- ☐ A first-generation packet-filtering firewall
- ☐ A circuit-level gateway
- ☐ An application-layer gateway, or proxy firewall, and stateful-inspection firewalls
- ☐ An application-layer gateway, or proxy firewall, but not stateful-inspection firewalls

Question 291

A transaction journal provides the information necessary for detecting unauthorized _____ (fill in the blank) from a terminal.

- ☐ Deletion
- ☐ Input
- ☐ Access
- ☐ Duplication

Question 292

Who is ultimately responsible and accountable for reviewing user access to systems?

- ☐ Systems security administrators
- ☐ Data custodians
- ☐ Data owners
- ☐ Information systems auditors

Question 293

When conducting a penetration test of an organization's internal network, which of the following approaches would BEST enable the conductor of the test to remain undetected on the network?

- ☐ Use the IP address of an existing file server or domain controller.
- ☐ Pause the scanning every few minutes to allow thresholds to reset.
- ☐ Conduct the scans during evening hours when no one is logged-in.
- ☐ Use multiple scanning tools since each tool has different characteristics.

Question 294

Which of the following would contribute MOST to an effective business continuity plan (BCP)?

- ☐ Document is circulated to all interested parties
- ☐ Planning involves all user departments
- ☐ Approval by senior management
- ☐ Audit by an external IS auditor

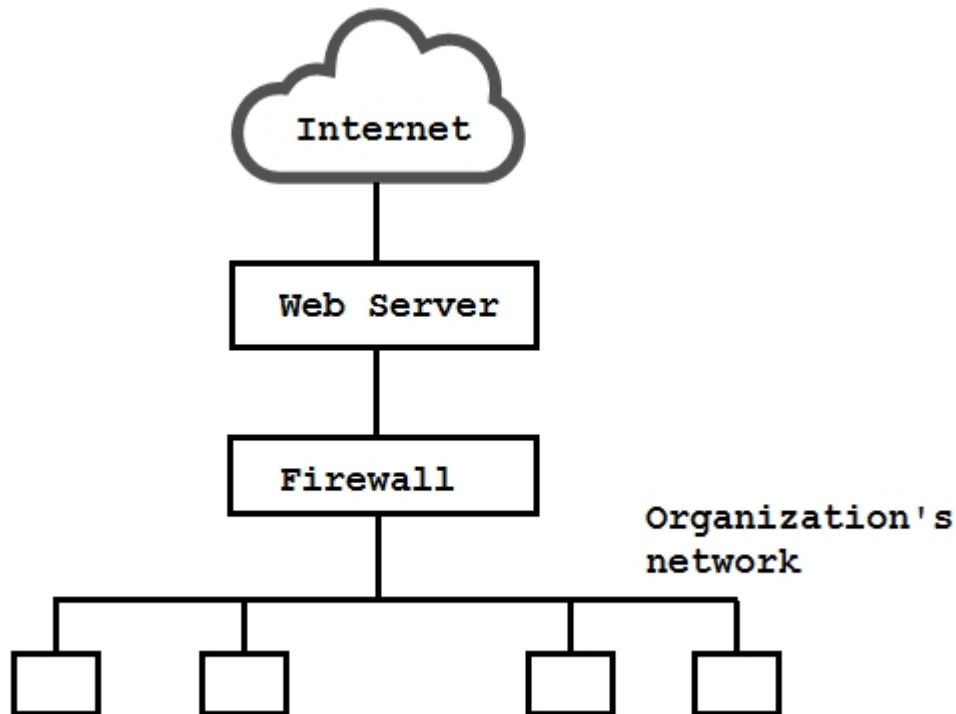
Question 295

Which of the following types of testing would determine whether a new or modifies system can operate in its target environment without adversely impacting other existing systems?

- ☐ Parallel testing
- ☐ Pilot testing
- ☐ Interface/integration testing
- ☐ Sociability testing

Question 296

To detect attack attempts that the firewall is unable to recognize, an IS auditor should recommend placing a network intrusion detection system (IDS) between the:



- ☐ Firewall and the organization's network.
- ☐ Internet and the firewall.
- ☐ Internet and the web server.
- ☐ Web server and the firewall.

Question 297

While conducting an audit, an IS auditor detects the presence of a virus. What should be the IS auditor's next step?

- ☐ Observe the response mechanism.
- ☐ Clear the virus from the network.
- ☐ Inform appropriate personnel immediately.
- ☐ Ensure deletion of the virus.

Question 298

What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

- ☐ The processes of the external agency should be subjected to an IS audit by an independent agency.
- ☐ Employees of the external agency should be trained on the security procedures of the organization.
- ☐ Any access by an external agency should be limited to the demilitarized zone (DMZ).
- ☐ The organization should conduct a risk assessment and design and implement appropriate controls.

Question 299

Which of the following type of lock uses a numeric keypad or dial to gain entry?

- ☐ Bolting door locks
- ☐ Cipher lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 300

During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:

- ☐ buffer overflow.
- ☐ brute force attack.
- ☐ distributed denial-of-service attack.
- ☐ war dialing attack.

Question 301

From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

- ☐ a big bang deployment after proof of concept.
- ☐ prototyping and a one-phase deployment.
- ☐ a deployment plan based on sequenced phases.
- ☐ to simulate the new infrastructure before deployment.

Question 302

Who is responsible for authorizing access level of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 303

A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?

- ☐ Badge readers are installed in locations where tampering would be noticed
- ☐ The computer that controls the badge system is backed up frequently
- ☐ A process for promptly deactivating lost or stolen badges exists
- ☐ All badge entry attempts are logged

Question 304

The optimum business continuity strategy for an entity is determined by the:

- ☐ lowest downtime cost and highest recovery cost.
- ☐ lowest sum of downtime cost and recovery cost.
- ☐ lowest recovery cost and highest downtime cost.
- ☐ average of the combined downtime and recovery cost.

Question 305

Which of the following BEST describes the role of a directory server in a public key infrastructure (PKI)?

- ☐ Encrypts the information transmitted over the network
- ☐ Makes other users' certificates available to applications
- ☐ Facilitates the implementation of a password policy
- ☐ Stores certificate revocation lists (CRLs)

Question 306

In which of the following WAN message transmission technique messages are divided into packets before they are sent and each packet is then transmitted individually and can even follow different routes to its destination?

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Question 307

When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- ☐ they are set to meet security and performance requirements.
- ☐ changes are recorded in an audit trail and periodically reviewed.
- ☐ changes are authorized and supported by appropriate documents.
- ☐ access to parameters in the system is restricted.

Question 308

Which of the following methods of suppressing a fire in a data center is the MOST effective and environmentally friendly?

- ☐ Halon gas
- ☐ Wet-pipe sprinklers
- ☐ Dry-pipe sprinklers
- ☐ Carbon dioxide gas

Question 309

Which of the following types of attack almost always requires physical access to the targets?

- ☐ Direct access attack
- ☐ Wireless attack
- ☐ Port attack
- ☐ Window attack
- ☐ System attack
- ☐ None of the choices.

Question 310

Over the long term, which of the following has the greatest potential to improve the security incident response process?

- ☐ A walkthrough review of incident response procedures
- ☐ Postevent reviews by the incident response team
- ☐ Ongoing security training for users
- ☐ Documenting responses to an incident

Question 311

Which of the following would BEST provide assurance of the integrity of new staff?

- ☐ background screening
- ☐ References
- ☐ Bonding
- ☐ Qualifications listed on a resume

Question 312

Obtaining user approval of program changes is very effective for controlling application changes and maintenance. True or false?

- ☐ True
- ☐ False

Question 313

What is the BEST approach to mitigate the risk of a phishing attack?

- ☐ implement an intrusion detection system (IDS)
- ☐ Assess web site security
- ☐ Strong authentication
- ☐ User education

Question 314

The majority of software vulnerabilities result from a few known kinds of coding defects, such as (choose all that apply):

- ☐ buffer overflows
- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Question 315

Talking about the different approaches to security in computing, the principle of regarding the computer system itself as largely an untrusted system emphasizes:

- ☐ most privilege
- ☐ full privilege
- ☐ least privilege
- ☐ null privilege
- ☐ None of the choices.

Question 316

An IS auditor inspected a windowless room containing phone switching and networking equipment and documentation binders. The room was equipped with two handheld fire extinguishers-one filled with CO₂, the other filled with halon. Which of the following should be given the HIGHEST priority in the auditor's report?

- ☐ The halon extinguisher should be removed because halon has a negative impact on the atmospheric ozone layer.
- ☐ Both fire suppression systems present a risk of suffocation when used in a closed room.
- ☐ The CO₂ extinguisher should be removed, because CO₂ is ineffective for suppressing fires involving solid combustibles (paper).
- ☐ The documentation binders should be removed from the equipment room to reduce potential risks.

Question 317

An IS auditor identifies that reports on product profitability produced by an organization's finance and marketing departments give different results. Further investigation reveals that the product definition being used by the two departments is different. What should the IS auditor recommend?

- ☐ User acceptance testing (UAT) occur for all reports before release into production
- ☐ Organizational data governance practices be put in place
- ☐ Standard software tools be used for report development
- ☐ Management sign-off on requirements for new reports

Question 318

Which of the following would provide the BEST protection against the hacking of a computer connected to the Internet?

- ☐ A remote access server
- ☐ A proxy server
- ☐ A personal firewall
- ☐ A password-generating token

Question 319

Which of the following would be BEST prevented by a raised floor in the computer machine room?

- ☐ Damage of wires around computers and servers
- ☐ A power failure from static electricity
- ☐ Shocks from earthquakes
- ☐ Water flood damage.

Question 320

Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

- ☐ downtime costs.
- ☐ resumption costs.
- ☐ recovery costs.
- ☐ walkthrough costs.

Question 321

During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

- ☐ Evacuation plan
- ☐ Recovery priorities
- ☐ Backup storages
- ☐ Call tree

Question 322

Which of the following is the INCORRECT Layer to Protocol mapping used in the DOD TCP/IP model?

- ☐ Application layer – Telnet
- ☐ Transport layer – ICMP
- ☐ Internet layer – IP
- ☐ Network Access layer – Ethernet

Question 323

Which of the following online auditing techniques is most effective for the early detection of errors or irregularities?

- ☐ Embedded audit module
- ☐ Integrated test facility
- ☐ Snapshots
- ☐ Audit hooks

Question 324

Which of the following is a benefit of using callback devices?

- ☐ Provide an audit trail
- ☐ Can be used in a switchboard environment
- ☐ Permit unlimited user mobility
- ☐ Allow call forwarding

Question 325

Which of the following technique is used for speeding up network traffic flow and making it easier to manage?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ MPLS
- ☐ ISDN

Question 326

Which of the following is an environmental issue caused by electric storms or noisy electric equipment and may also cause computer system to hang or crash?

- ☐ Sag
- ☐ Blackout
- ☐ Brownout
- ☐ EMI

Question 327

The MOST significant level of effort for business continuity planning (BCP) generally is required during the:

- ☐ testing stage.
- ☐ evaluation stage.
- ☐ maintenance stage.
- ☐ early stages of planning.

Question 328

Data flow diagrams are used by IS auditors to:

- ☐ order data hierarchically.
- ☐ highlight high-level data definitions.
- ☐ graphically summarize data paths and storage.
- ☐ portray step-by-step details of data generation.

Question 329

The MAJOR advantage of the risk assessment approach over the baseline approach to information security management is that it ensures:

- ☐ information assets are overprotected.
- ☐ a basic level of protection is applied regardless of asset value.
- ☐ appropriate levels of protection are applied to information assets.
- ☐ an equal proportion of resources are devoted to protecting all information assets.

Question 330

Structured programming is BEST described as a technique that:

- ☐ provides knowledge of program functions to other programmers via peer reviews.
- ☐ reduces the maintenance time of programs by the use of small-scale program modules.
- ☐ makes the readable coding reflect as closely as possible the dynamic execution of the program.
- ☐ controls the coding and testing of the high-level functions of the program in the development process.

Question 331

For which of the following applications would rapid recovery be MOST crucial?

- ☐ Point-of-sale system
- ☐ Corporate planning
- ☐ Regulatory reporting
- ☐ Departmental chargeback

Question 332

During the audit of a database server, which of the following would be considered the GREATEST exposure?

- ☐ The password does not expire on the administrator account
- ☐ Default global security settings for the database remain unchanged
- ☐ Old data have not been purged
- ☐ Database activity is not fully logged

Question 333

In planning an audit, the MOST critical step is the identification of the:

- ☐ areas of high risk.
- ☐ skill sets of the audit staff.
- ☐ test steps in the audit.
- ☐ time allotted for the audit.

Question 334

How is the risk of improper file access affected upon implementing a database system?

- ☐ Risk varies.
- ☐ Risk is reduced.
- ☐ Risk is not affected.
- ☐ Risk is increased.

Question 335

The MOST effective biometric control system is the one:

- ☐ which has the highest equal-error rate (EER).
- ☐ which has the lowest EER.
- ☐ for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- ☐ for which the FRR is equal to the failure-to-enroll rate (FER).

Question 336

An efficient use of public key infrastructure (PKI) should encrypt the:

- ☐ entire message.
- ☐ private key.
- ☐ public key.
- ☐ symmetric session key.

Question 337

Which of the following level in CMMI model focuses on process innovation and continuous optimization?

- ☐ Level 4
- ☐ Level 5
- ☐ Level 3
- ☐ Level 2

Question 338

Which of the following is a passive attack to a network?

- ☐ Message modification
- ☐ Masquerading
- ☐ Denial of service
- ☐ Traffic analysis

Question 339

Which of the following protocol uses serial interface for communication between two computers in WAN technology?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ Frame Relay
- ☐ ISDN

Question 340

An auditor needs to be aware of technical controls which are used to protect computer from malware. Which of the following technical control interrupts DoS and ROM BIOS call and look for malware like action?

- ☐ Scanners
- ☐ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Question 341

Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?

- ☐ System analysis
- ☐ Authorization of access to data
- ☐ Application programming
- ☐ Data administration

Question 342

An IS steering committee should:

- ☐ include a mix of members from different departments and staff levels.
- ☐ ensure that IS security policies and procedures have been executed properly.
- ☐ have formal terms of reference and maintain minutes of its meetings.
- ☐ be briefed about new trends and products at each meeting by a vendor.

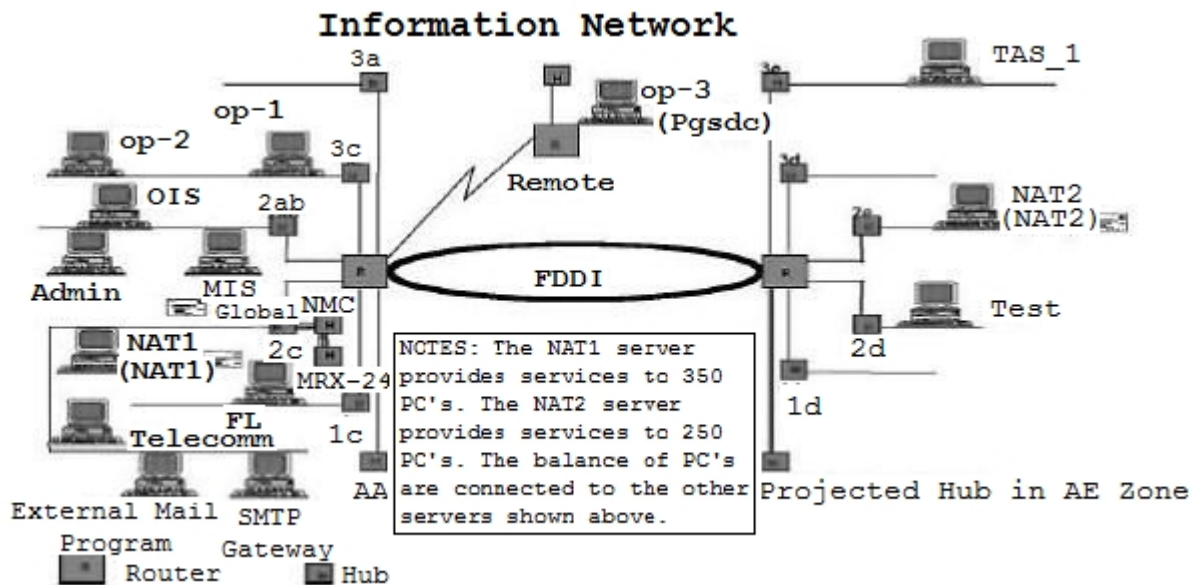
Question 343

Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?

- ☐ Achieve standards alignment through an increase of resources devoted to the project
- ☐ Align the data definition standards after completion of the project
- ☐ Delay the project until compliance with standards can be achieved
- ☐ Enforce standard compliance by adopting punitive measures against violators

Question 344

For locations 3a, 1d and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?



- ☐ Intelligent hub
- ☐ Physical security over the hubs
- ☐ Physical security and an intelligent hub
- ☐ No controls are necessary since this is not a weakness

Question 345

Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- ☐ Firewalls
- ☐ Routers
- ☐ Layer 2 switches
- ☐ VLANs

Question 346

Which of the following would be the BEST method for ensuring that critical fields in a master record have been updated properly?

- ☐ Field checks
- ☐ Control totals
- ☐ Reasonableness checks
- ☐ A before-and-after maintenance report

Question 347

How does the SSL network protocol provide confidentiality?

- ☐ Through symmetric encryption such as RSA
- ☐ Through asymmetric encryption such as Data Encryption Standard, or DES
- ☐ Through asymmetric encryption such as Advanced Encryption Standard, or AES
- ☐ Through symmetric encryption such as Data Encryption Standard, or DES

Question 348

Which of the following service is a distributed database that translate host name to IP address to IP address to host name?

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Question 349

Accountability for the maintenance of appropriate security measures over information assets resides with the:

- ☐ security administrator.
- ☐ systems administrator.
- ☐ data and systems owners.
- ☐ systems operations group.

Question 350

Which of the following testing method examines the functionality of an application without peering into its internal structure or knowing the details of it's internals?

- ☐ Black-box testing
- ☐ Parallel Test
- ☐ Regression Testing
- ☐ Pilot Testing

Question 351

The management of an organization has decided to establish a security awareness program. Which of the following would MOST likely be a part of the program?

- ☐ Utilization of an intrusion detection system to report incidents
- ☐ Mandating the use of passwords to access all software
- ☐ Installing an efficient user log system to track the actions of each user
- ☐ Training provided on a regular basis to all current and new employees

Question 352

Which of the following protocol is developed jointly by VISA and Master Card to secure payment transactions among all parties involved in credit card transactions on behalf of cardholders and merchants?

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

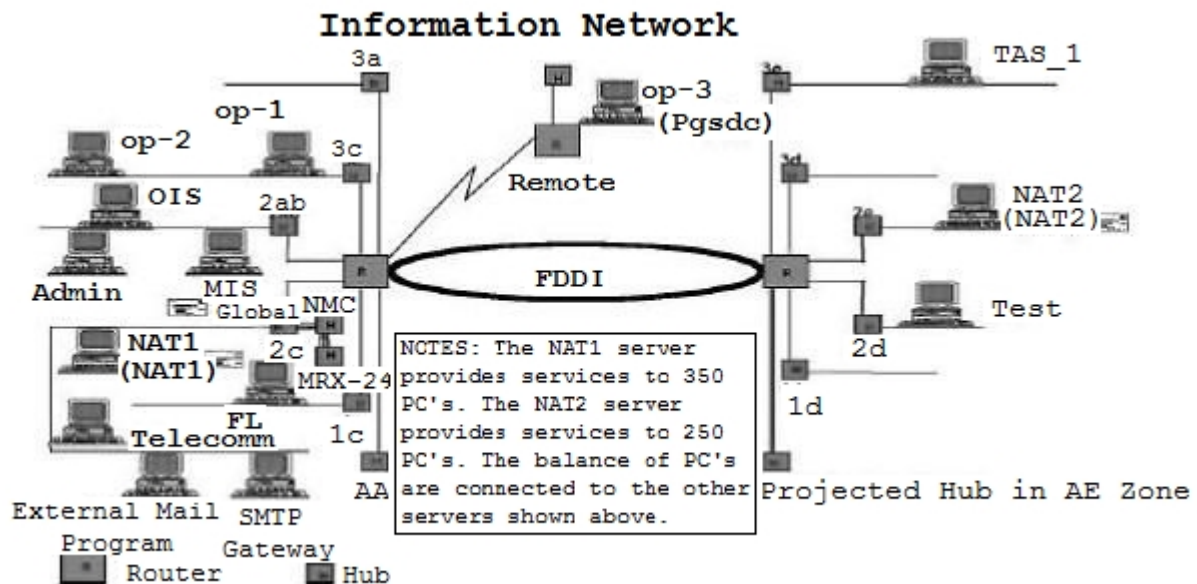
Question 353

What is used to provide authentication of the website and can also be used to successfully authenticate keys used for data encryption?

- ☐ An organizational certificate
- ☐ A user certificate
- ☐ A website certificate
- ☐ Authenticode

Question 354

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?



- ☐ No firewalls are needed
- ☐ Op-3 location only
- ☐ MIS (Global) and NAT2
- ☐ SMTP Gateway and op-3

Question 355

The ultimate purpose of IT governance is to:

- ☐ encourage optimal use of IT.
- ☐ reduce IT costs.
- ☐ decentralize IT resources across the organization.
- ☐ centralize control of IT.

Question 356

An IS auditor reviewing a proposed application software acquisition should ensure that the:

- ☐ operating system (OS) being used is compatible with the existing hardware platform.
- ☐ planned OS updates have been scheduled to minimize negative impacts on company needs.
- ☐ OS has the latest versions and updates.
- ☐ products are compatible with the current or planned OS.

Question 357

A control that detects transmission errors by appending calculated bits onto the end of each segment of data is known as a:

- ☐ reasonableness check.
- ☐ parity check.
- ☐ redundancy check.
- ☐ check digits.

Question 358

Which of the following attack occurs when a malicious action is performed by invoking the operating system to execute a particular system call?

- ☐ Eavesdropping
- ☐ Traffic analysis
- ☐ Masquerading
- ☐ Interrupt attack

Question 359

What influences decisions regarding criticality of assets?

- ☐ The business criticality of the data to be protected
- ☐ Internal corporate politics
- ☐ The business criticality of the data to be protected, and the scope of the impact upon the organization as a whole
- ☐ The business impact analysis

Question 360

Which of the following encryption techniques will BEST protect a wireless network from a man-in-the-middle attack?

- ☐ 128-bit wired equivalent privacy (WEP)
- ☐ MAC-based pre-shared key (PSK)
- ☐ Randomly generated pre-shared key (PSK)
- ☐ Alphanumeric service set identifier (SSID)

Question 361

Which of the following property of the core data warehouse layer of an enterprise data flow architecture uses common attributes to access a cross section of an information in the warehouse?

- ☐ Drill up
- ☐ Drill down
- ☐ Drill across
- ☐ Historical Analysis

Question 362

Which of the following provides the BEST single-factor authentication?

- ☐ Biometrics
- ☐ Password
- ☐ Token
- ☐ PIN

Question 363

Users are issued security tokens to be used in combination with a PIN to access the corporate virtual private network (VPN). Regarding the PIN, what is the MOST important rule to be included in a security policy?

- ☐ Users should not leave tokens where they could be stolen
- ☐ Users must never keep the token in the same bag as their laptop computer
- ☐ Users should select a PIN that is completely random, with no repeating digits
- ☐ Users should never write down their PIN

Question 364

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. True or false?

- ☐ True
- ☐ False

Question 365

When selecting audit procedures, an IS auditor should use professional judgment to ensure that:

- ☐ sufficient evidence will be collected.
- ☐ all significant deficiencies identified will be corrected within a reasonable period.
- ☐ all material weaknesses will be identified.
- ☐ audit costs will be kept at a minimum level.

Question 366

Which of the following types of data validation editing checks is used to determine if a field contains data, and not zeros or blanks?

- ☐ Check digit
- ☐ Existence check
- ☐ Completeness check
- ☐ Reasonableness check

Question 367

A database administrator is responsible for:

- ☐ defining data ownership.
- ☐ establishing operational standards for the data dictionary.
- ☐ creating the logical and physical database.
- ☐ establishing ground rules for ensuring data integrity and security.

Question 368

Company.com has contracted with an external consulting firm to implement a commercial financial system to replace its existing in-house developed system. In reviewing the proposed development approach, which of the following would be of GREATEST concern?

- ☐ Acceptance testing is to be managed by users.
- ☐ A quality plan is not part of the contracted deliverables.
- ☐ Not all business functions will be available on initial implementation.
- ☐ Prototyping is being used to confirm that the system meets business requirements.

Question 369

Which of the following is the MOST effective control over visitor access to a data center?

- ☐ Visitors are escorted.
- ☐ Visitor badges are required.
- ☐ Visitors sign in.
- ☐ Visitors are spot-checked by operators.

Question 370

When participating in a systems-development project, an IS auditor should focus on system controls rather than ensuring that adequate and complete documentation exists for all projects. True or false?

- ☐ True
- ☐ False

Question 371

After initial investigation, an IS auditor has reasons to believe that fraud may be present. The IS auditor should:

- ☐ expand activities to determine whether an investigation is warranted
- ☐ report the matter to the audit committee.
- ☐ report the possibility of fraud to top management and ask how they would like to be proceed.
- ☐ consult with external legal counsel to determine the course of action to be taken.

Question 372

Which of the following refers to a method of bypassing normal system authentication procedures?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ backdoor
- ☐ None of the choices.

Question 373

Identify the correct sequence which needs to be followed as a chain of event in regards to evidence handling in computer forensics?

- ☐ Identify, Analyze, preserve and Present
- ☐ Analyze, Identify, preserve and present
- ☐ Preserve, Identify, Analyze and Present
- ☐ Identify, Preserve, Analyze and Present

Question 374

Which of the following method should be recommended by security professional to erase the data on the magnetic media that would be reused by another employee?

- ☐ Degaussing
- ☐ Overwrite every sector of magnetic media with pattern of 1's and 0's
- ☐ Format magnetic media
- ☐ Delete File allocation table

Question 375

During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

- ☐ Storage area network (SAN)
- ☐ Network Attached Storage (NAS)
- ☐ Network file system (NFS v2)
- ☐ Common Internet File System (CIFS)

Question 376

Which of the following layer of an enterprise data flow architecture is concerned with basic data communication?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Internet/Intranet layer
- ☐ Data access layer

Question 377

Which of the following term in business continuity determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 378

An IS auditor reviewing wireless network security determines that the Dynamic Host Configuration Protocol is disabled at all wireless access points. This practice:

- ☐ reduces the risk of unauthorized access to the network.
- ☐ is not suitable for small networks.
- ☐ automatically provides an IP address to anyone.
- ☐ increases the risks associated with Wireless Encryption Protocol (WEP).

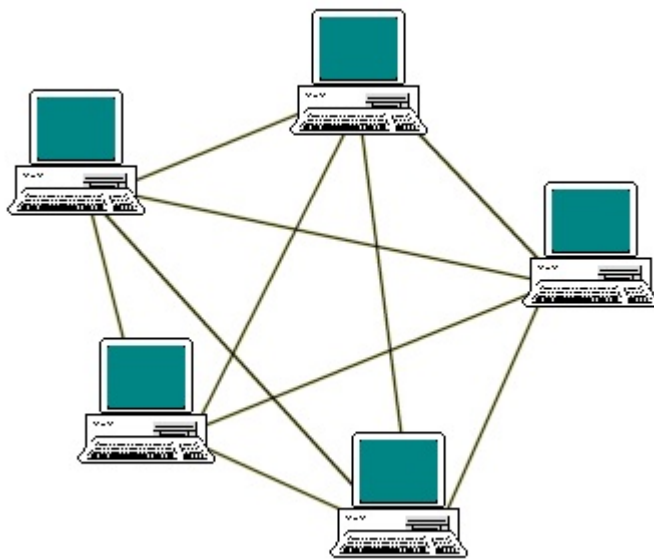
Question 379

To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

- ☐ business software.
- ☐ infrastructure platform tools.
- ☐ application services.
- ☐ system development tools.

Question 380

Identify the network topology from below diagram presented below:



Network Topology

- ☐ Bus
- ☐ Star
- ☐ Ring
- ☐ Mesh

Question 381

Ensuring that security and control policies support business and IT objectives is a primary objective of:

- ☐ An IT security policies audit
- ☐ A processing audit
- ☐ A software audit
- ☐ A vulnerability assessment

Question 382

Which of the following type of computer has highest processing speed?

- ☐ Supercomputers
- ☐ Midrange servers
- ☐ Personal computers
- ☐ Thin client computers

Question 383

In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- ☐ Diskless workstations
- ☐ Data encryption techniques
- ☐ Network monitoring devices
- ☐ Authentication systems

Question 384

Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?

- ☐ Pilot
- ☐ Paper
- ☐ Unit
- ☐ System

Question 385

The success of control self-assessment (CSA) highly depends on:

- ☐ having line managers assume a portion of the responsibility for control monitoring.
- ☐ assigning staff managers the responsibility for building, but not monitoring, controls.
- ☐ the implementation of a stringent control policy and rule-driven controls.
- ☐ the implementation of supervision and the monitoring of controls of assigned duties.

Question 386

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?

- ☐ increase the time allocated for system testing
- ☐ implement formal software inspections
- ☐ increase the development staff
- ☐ Require the sign-off of all project deliverables

Question 387

When are benchmarking partners identified within the benchmarking process?

- ☐ In the design stage
- ☐ In the testing stage
- ☐ In the research stage
- ☐ In the development stage

Question 388

Which of the following attacks could capture network user passwords?

- ☐ Data diddling
- ☐ Sniffing
- ☐ IP Spoofing
- ☐ Surfing

Question 389

In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- ☐ address of the domain server.
- ☐ resolution service for the name/address.
- ☐ IP addresses for the internet.
- ☐ domain name system.

Question 390

John had implemented a validation check on the marital status field of a payroll record. A payroll record contains a field for marital status and acceptable status code are M for Married or S for Single. If any other code is entered, record should be rejected. Which of the following data validation control was implemented by John?

- ☐ Range Check
- ☐ Validity Check
- ☐ Existence check
- ☐ Reasonableness check

Question 391

The extent to which data will be collected during an IS audit should be determined based on the:

- ☐ availability of critical and required information.
- ☐ auditor's familiarity with the circumstances.
- ☐ auditee's ability to find relevant evidence.
- ☐ purpose and scope of the audit being done.

Question 392

An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?

- ☐ Use a process-based maturity model such as the capability maturity model (CMM)
- ☐ Regular monitoring of task-level progress against schedule
- ☐ Extensive use of software development tools to maximize team productivity
- ☐ Postiteration reviews that identify lessons learned for future use in the project

Question 393

A computer system is no more secure than the human systems responsible for its operation. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals, or by deliberately deceiving them. zombie computers are being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Question 394

Why is one-time pad not always preferable for encryption (choose all that apply):

- ☐ it is difficult to use securely.
- ☐ it is highly inconvenient to use.
- ☐ it requires licensing fee.
- ☐ it requires internet connectivity.
- ☐ it is Microsoft only.
- ☐ None of the choices.

Question 395

Which of the following types of firewalls would BEST protect a network from an internet attack?

- ☐ Screened subnet firewall
- ☐ Application filtering gateway
- ☐ Packet filtering router
- ☐ Circuit-level gateway

Question 396

During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:

- ☐ increased maintenance.
- ☐ improper documentation of testing.
- ☐ inadequate functional testing.
- ☐ delays in problem resolution.

Question 397

The waterfall life cycle model of software development is most appropriately used when:

- ☐ requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate.
- ☐ requirements are well understood and the project is subject to time pressures.
- ☐ the project intends to apply an object-oriented design and programming approach.
- ☐ the project will involve the use of new technology.

Question 398

Which of the following antispam filtering techniques would BEST prevent a valid, variable-length e-mail message containing a heavily weighted spam keyword from being labeled as spam?

- ☐ Heuristic (rule-based)
- ☐ Signature-based
- ☐ Pattern matching
- ☐ Bayesian (statistical)

Question 399

When auditing security for a data center, an IS auditor should look for the presence of a voltage regulator to ensure that the:

- ☐ hardware is protected against power surges.
- ☐ integrity is maintained if the main power is interrupted.
- ☐ immediate power will be available if the main power is lost.
- ☐ hardware is protected against long-term power fluctuations.

Question 400

Which of the following device in Frame Relay WAN technique is generally customer owned device that provides a connectivity between company's own network and the frame relays network?

- ☐ DTE
- ☐ DCE
- ☐ DME
- ☐ DLE

Question 401

Which of the following type of testing validate functioning of the application under test with other system, where a set of data is transferred from one system to another?

- ☐ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Question 402

An organization is using symmetric encryption. Which of the following would be a valid reason for moving to asymmetric encryption? Symmetric encryption:

- ☐ provides authenticity.
- ☐ is faster than asymmetric encryption.
- ☐ can cause key management to be difficult.
- ☐ requires a relatively simple algorithm.

Question 403

The PRIMARY objective of implementing corporate governance by an organization's management is to:

- ☐ provide strategic direction.
- ☐ control business operations.
- ☐ align IT with business.
- ☐ implement best practices.

Question 404

IS management has decided to rewrite a legacy customer relations system using fourth generation languages (4GLs). Which of the following risks is MOST often associated with system development using 4GLs?

- ☐ Inadequate screen/report design facilities
- ☐ Complex programming language subsets
- ☐ Lack of portability across operating systems
- ☐ Inability to perform data intensive operations

Question 405

A retail outlet has introduced radio frequency identification (RFID) tags to create unique serial numbers for all products. Which of the following is the PRIMARY concern associated with this initiative?

- ☐ Issues of privacy
- ☐ Wavelength can be absorbed by the human body
- ☐ RFID tags may not be removable
- ☐ RFID eliminates line-of-sight reading

Question 406

An IS auditor performing a review of an application's controls would evaluate the:

- ☐ efficiency of the application in meeting the business processes.
- ☐ impact of any exposures discovered.
- ☐ business processes served by the application.
- ☐ application's optimization.

Question 407

An IS auditor evaluating logical access controls should FIRST:

- ☐ document the controls applied to the potential access paths to the system.
- ☐ test controls over the access paths to determine if they are functional.
- ☐ evaluate the security environment in relation to written policies and practices
- ☐ obtain an understanding of the security risks to information processing.

Question 408

What type of fire-suppression system suppresses fire via water that is released from a main valve to be delivered via a system of dry pipes installed throughout the facilities?

- ☐ A dry-pipe sprinkler system
- ☐ A deluge sprinkler system
- ☐ A wet-pipe system
- ☐ A halon sprinkler system

Question 409

A penetration test performed as part of evaluating network security:

- ☐ provides assurance that all vulnerabilities are discovered.
- ☐ should be performed without warning the organization's management.
- ☐ exploits the existing vulnerabilities to gain unauthorized access.
- ☐ would not damage the information assets when performed at network perimeters.

Question 410

Which of the following statement is NOT true about smoke detector?

- ☐ The Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised in the computer room floor
- ☐ The smoke detector should produce an audible alarm when activated and be linked to a monitored station
- ☐ The location of the smoke detector should be marked on the tiling for easy identification and access
- ☐ Smoke detector should replace fire suppression system

Question 411

Which of the following is an estimation technique where the results can be measure by the functional size of an information system based on the number and complexity of input, output, interface and queries?

- ☐ Functional Point analysis
- ☐ Gantt Chart
- ☐ Time box management
- ☐ Critical path methodology

Question 412

Why is the WAP gateway a component warranting critical concern and review for the IS auditor when auditing and testing controls enforcing message confidentiality?

- ☐ WAP is often configured by default settings and is thus insecure.
- ☐ WAP provides weak encryption for wireless traffic.
- ☐ WAP functions as a protocol-conversion gateway for wireless TLS to Internet SSL.
- ☐ WAP often interfaces critical IT systems.

Question 413

TEMPEST is a hardware for which of the following purposes?

- ☐ Eavedropping
- ☐ Social engineering
- ☐ Virus scanning
- ☐ Firewalling
- ☐ None of the choices.

Question 414

If an IS auditor observes that an IS department fails to use formal documented methodologies, policies, and standards, what should the auditor do?

- ☐ Lack of IT documentation is not usually material to the controls tested in an IT audit.
- ☐ The auditor should at least document the informal standards and policies. Furthermore, the IS auditor should create formal documented policies to be implemented.
- ☐ The auditor should at least document the informal standards and policies, and test for a compliance. Furthermore, the IS auditor should recommend management that formal documented policies be developed and implemented.
- ☐ The auditor should at least document the informal standards and policies, and test for compliance. Furthermore, the IS auditor should create formal documented policies to be implemented.

Question 415

What is a risk associated with attempting to control physical access to sensitive areas such as computer rooms using card keys or locks?

- ☐ Unauthorized individuals wait for controlled doors to open and walk in behind those authorized.
- ☐ The contingency plan for the organization cannot effectively test controlled access practices.
- ☐ Access cards, keys and pads can be easily duplicated allowing easy compromise of the control.
- ☐ Removing access for those who are no longer authorized is complex.

Question 416

Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- ☐ Palm scan
- ☐ Face recognition
- ☐ Retina scan
- ☐ Hand geometry

Question 417

An audit charter should:

- ☐ be dynamic and change often to coincide with the changing nature of technology and the audit profession.
- ☐ clearly state audit objectives for, and the delegation of, authority to the maintenance and review of internal controls.
- ☐ document the audit procedures designed to achieve the planned audit objectives.
- ☐ outline the overall authority, scope and responsibilities of the audit function.

Question 418

Which of the following term in business continuity determines the maximum tolerable amount of time needed to bring all critical systems back online after disaster occurs?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 419

To address a maintenance problem, a vendor needs remote access to a critical network. The MOST secure and effective solution is to provide the vendor with a:

- ☐ Secure Shell (SSH-2) tunnel for the duration of the problem.
- ☐ two-factor authentication mechanism for network access.
- ☐ dial-in access.
- ☐ virtual private network (VPN) account for the duration of the vendor support contract.

Question 420

Which of the following type of testing has two major categories: QAT and UAT?

- ☐ Interface testing
- ☐ Unit Testing
- ☐ System Testing
- ☐ Final acceptance testing

Question 421

Which of the following is MOST likely to result from a business process reengineering (BPR) Project?

- ☐ An increased number of people using technology
- ☐ Significant cost saving, through a reduction the complexity of information technology
- ☐ A weaker organizational structures and less accountability
- ☐ Increased information protection (IP) risk will increase

Question 422

Active radio frequency ID (RFID) tags are subject to which of the following exposures?

- ☐ Session hijacking
- ☐ Eavesdropping
- ☐ Malicious code
- ☐ Phishing

Question 423

Which of the following PBX feature allows a PBX to be configured so that incoming calls are distributed to the next available agent or placed on-hold until one become available?

- ☐ Automatic Call distribution
- ☐ Call forwarding
- ☐ Tenanting
- ☐ Voice mail

Question 424

The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

- ☐ Contact information of key personnel
- ☐ Server inventory documentation
- ☐ individual roles and responsibilities
- ☐ Procedures for declaring a disaster

Question 425

What is an edit check to determine whether a field contains valid data?

- ☐ Completeness check
- ☐ Accuracy check
- ☐ Redundancy check
- ☐ Reasonableness check

Question 426

Back Orifice is an example of:

- ☐ a virus.
- ☐ a legitimate remote control software.
- ☐ a backdoor that takes the form of an installed program.
- ☐ an eavesdropper.
- ☐ None of the choices.

Question 427

Of the three major types of off-site processing facilities, what type is often an acceptable solution for preparing for recovery of noncritical systems and data?

- ☐ Cold site
- ☐ Hot site
- ☐ Alternate site
- ☐ Warm site

Question 428

Which of the following is the PRIMARY purpose for conducting parallel testing?

- ☐ To determine if the system is cost-effective
- ☐ To enable comprehensive unit and system testing
- ☐ To highlight errors in the program interfaces with files
- ☐ To ensure the new system meets user requirements

Question 429

While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:

- ☐ shadow file processing.
- ☐ electronic vaulting.
- ☐ hard-disk mirroring.
- ☐ hot-site provisioning.

Question 430

Which of the following PBX feature provides the possibility to break into a busy line to inform another user of an important message?

- ☐ Account Codes
- ☐ Access Codes
- ☐ Override
- ☐ Tenanting

Question 431

After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?

- ☐ Perform an integral review of the recovery tasks.
- ☐ Broaden the processing capacity to gain recovery time.
- ☐ Make improvements in the facility's circulation structure.
- ☐ increase the amount of human resources involved in the recovery.

Question 432

Which of the following statement INCORRECTLY describes device and where they sit within the TCP/IP model?

- ☐ Layer 4 switch work at Network interface layer in TCP/IP model
- ☐ Router works at Network interface layer in TCP/IP model
- ☐ Layer 3 switch work at Network interface layer in TCP/IP model
- ☐ Hub works at LAN or WAN interface layer of a TCP/IP model

Question 433

The IS auditor learns that when equipment was brought into the data center by a vendor, the emergency power shutoff switch was accidentally pressed and the UPS was engaged. Which of the following audit recommendations should the IS auditor suggest?

- ☐ Relocate the shut off switch.
- ☐ Install protective covers.
- ☐ Escort visitors.
- ☐ Log environmental failures.

Question 434

An organization has contracted with a vendor for a turnkey solution for their electronic toll collection system (ETCS). The vendor has provided its proprietary application software as part of the solution. The contract should require that:

- ☐ a backup server be available to run ETCS operations with up-to-date data.
- ☐ a backup server be loaded with all the relevant software and data.
- ☐ the systems staff of the organization be trained to handle any event.
- ☐ source code of the ETCS application be placed in escrow.

Question 435

What is the recommended initial step for an IS auditor to implement continuous-monitoring systems?

- ☐ Document existing internal controls
- ☐ Perform compliance testing on internal controls
- ☐ Establish a controls-monitoring steering committee
- ☐ Identify high-risk areas within the organization

Question 436

Which of the following ensures confidentiality of information sent over the internet?

- ☐ Digital signature
- ☐ Digital certificate
- ☐ Online Certificate Status Protocol
- ☐ Private key cryptosystem

Question 437

Which of the following is an oft-cited cause of vulnerability of networks?

- ☐ software monoculture
- ☐ software diversification
- ☐ single line of defense
- ☐ multiple DMZ
- ☐ None of the choices.

Question 438

As compared to understanding an organization's IT process from evidence directly collected, how valuable are prior audit reports as evidence?

- ☐ The same value.
- ☐ Greater value.
- ☐ Lesser value.
- ☐ Prior audit reports are not relevant.

Question 439

Which of the following refers to an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer?

- ☐ buffer overflow
- ☐ format string vulnerabilities
- ☐ integer misappropriation
- ☐ code injection
- ☐ None of the choices.

Question 440

Which of the following BEST characterizes a mantrap or deadman door, which is used as a deterrent control for the vulnerability of piggybacking?

- ☐ A monitored double-doorway entry system
- ☐ A monitored turnstile entry system
- ☐ A monitored doorway entry system
- ☐ A one-way door that does not allow exit after entry

Question 441

Which are the two primary types of scanner used for protecting against Malware?

Malware mask/signatures and Heuristic Scanner

Active and passive Scanner

Behavioral Blockers and immunizer Scanner

None of the above

- ☐ Malware mask/signatures and Heuristic Scanner
- ☐ Active and passive Scanner
- ☐ Behavioral Blockers and immunizer Scanner
- ☐ None of the above

Question 442

Which of the following provides the strongest authentication for physical access control?

- ☐ Sign-in logs
- ☐ Dynamic passwords
- ☐ Key verification
- ☐ Biometrics

Question 443

In an EDI process, the device which transmits and receives electronic documents is the:

- ☐ communications handler.
- ☐ EDI translator.
- ☐ application interface.
- ☐ EDI interface.

Question 444

A financial services organization is developing and documenting business continuity measures. In which of the following cases would an IS auditor MOST likely raise an issue?

- ☐ The organization uses good practice guidelines instead of industry standards and relies on external advisors to ensure the adequacy of the methodology.
- ☐ The business continuity capabilities are planned around a carefully selected set of scenarios which describe events that might happen with a reasonable probability.
- ☐ The recovery time objectives (RTOs) do not take IT disaster recovery constraints into account, such as personnel or system dependencies during the recovery phase.
- ☐ The organization plans to rent a shared alternate site with emergency workplaces which has only enough room for half of the normal staff.

Question 445

Which of the following is the MOST important action in recovering from a cyberattack?

- ☐ Creation of an incident response team
- ☐ Use of cybenforensic investigators
- ☐ Execution of a business continuity plan
- ☐ Filling an insurance claim

Question 446

An offsite information processing facility having electrical wiring, air conditioning and flooring, but no computer or communications equipment is a:

- ☐ cold site.
- ☐ warm site.
- ☐ dial-up site.
- ☐ duplicate processing facility.

Question 447

Which of the following measures can effectively minimize the possibility of buffer overflows?

- ☐ Sufficient bounds checking
- ☐ Sufficient memory
- ☐ Sufficient processing capability
- ☐ Sufficient code injection
- ☐ None of the choices

Question 448

An IS auditor notes that IDS log entries related to port scanning are not being analyzed. This lack of analysis will MOST likely increase the risk of success of which of the following attacks?

- ☐ Denial-of-service
- ☐ Replay
- ☐ Social engineering
- ☐ Buffer overflow

Question 449

When reviewing the implementation of a LAN, an IS auditor should FIRST review the:

- ☐ node list.
- ☐ acceptance test report.
- ☐ network diagram.
- ☐ user's list.

Question 450

Which of the following can help detect transmission errors by appending specially calculated bits onto the end of each segment of data?

- ☐ Redundancy check
- ☐ Completeness check
- ☐ Accuracy check
- ☐ Parity check

Question 451

Which of the following attack is against computer network and involves fragmented or invalid ICMP packets sent to the target?

- ☐ Nuke attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 452

How do modems (modulation/demodulation) function to facilitate analog transmissions to enter a digital network?

- ☐ Modems convert analog transmissions to digital, and digital transmission to analog.
- ☐ Modems encapsulate analog transmissions within digital, and digital transmissions within analog.
- ☐ Modems convert digital transmissions to analog, and analog transmissions to digital.
- ☐ Modems encapsulate digital transmissions within analog, and analog transmissions within digital.

Question 453

In which of the following payment mode, the payer creates payment transfer instructions, signs it digitally and sends it to issuer?

- ☐ Electronic Money Model
- ☐ Electronics Checks model
- ☐ Electronic transfer model
- ☐ Electronic withdraw model

Question 454

Which of the following would normally be the MOST reliable evidence for an auditor?

- ☐ A confirmation letter received from a third party verifying an account balance
- ☐ Assurance from line management that an application is working as designed
- ☐ Trend data obtained from World Wide Web (Internet) sources
- ☐ Ratio analysts developed by the IS auditor from reports supplied by line management

Question 455

The PRIMARY objective of an audit of IT security policies is to ensure that:

- ☐ they are distributed and available to all staff.
- ☐ security and control policies support business and IT objectives.
- ☐ there is a published organizational chart with functional descriptions.
- ☐ duties are appropriately segregated.

Question 456

Which of the following devices extends the network and has the capacity to store frames and act as a storage and forward device?

- ☐ Router
- ☐ Bridge
- ☐ Repeater
- ☐ Gateway

Question 457

Involvement of senior management is MOST important in the development of:

- ☐ strategic plans.
- ☐ IS policies.
- ☐ IS procedures.
- ☐ standards and guidelines.

Question 458

Responsibility for the governance of IT should rest with the:

- ☐ IT strategy committee.
- ☐ chief information officer (CIO).
- ☐ audit committee.
- ☐ board of directors.

Question 459

Which of the following BEST supports the prioritization of new IT projects?

- ☐ Internal control self-assessment (CSA)
- ☐ Information systems audit
- ☐ Investment portfolio analysis
- ☐ Business risk assessment

Question 460

The initial step in establishing an information security program is the:

- ☐ development and implementation of an information security standards manual.
- ☐ performance of a comprehensive security control review by the IS auditor.
- ☐ adoption of a corporate information security policy statement.
- ☐ purchase of security access control software.

Question 461

Which of the following would be the BEST population to take a sample from when testing program changes?

- ☐ Test library listings
- ☐ Source program listings
- ☐ Program change requests
- ☐ Production library listings

Question 462

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. The IS auditor should:

- ☐ create the procedures document.
- ☐ terminate the audit.
- ☐ conduct compliance testing.
- ☐ identify and evaluate existing practices.

Question 463

Which of the following INCORRECTLY describes the layer function of the Application Layer within the TCP/IP model?

- ☐ Provides user interface
- ☐ Perform data processing such as encryption, encoding, etc
- ☐ Provides reliable delivery
- ☐ Keeps separate the data of different applications

Question 464

Which of the following is a good control for protecting confidential data residing on a PC?

- ☐ Personal firewall
- ☐ File encapsulation
- ☐ File encryption
- ☐ Host-based intrusion detection

Question 465

During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:

- ☐ event error log generated at the disaster recovery site.
- ☐ disaster recovery test plan.
- ☐ disaster recovery plan (DRP).
- ☐ configurations and alignment of the primary and disaster recovery sites.

Question 466

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- ☐ nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- ☐ access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- ☐ card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- ☐ the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Question 467

In computer forensic which of the following describe the process that converts the information extracted into a format that can be understood by investigator?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Question 468

Which of the following statement correctly describes the differences between tunnel mode and transport mode of the IPSec protocol?

- ☐ In transport mode the ESP is encrypted where as in tunnel mode the ESP and its header's are encrypted
- ☐ In tunnel mode the ESP is encrypted where as in transport mode the ESP and its header's are encrypted
- ☐ In both modes (tunnel and transport mode) the ESP and its header's are encrypted
- ☐ There is no encryption provided when using ESP or AH

Question 469

Which of the following is by far the most common prevention system from a network security perspective?

- ☐ Firewall
- ☐ IDS
- ☐ IPS
- ☐ Hardened OS
- ☐ Tripwire
- ☐ None of the choices.

Question 470

Validated digital signatures in an e-mail software application will:

- ☐ help detect spam.
- ☐ provide confidentiality.
- ☐ add to the workload of gateway servers.
- ☐ significantly reduce available bandwidth.

Question 471

Which of the following typically focuses on making alternative processes and resources available for transaction processing?

- ☐ Cold-site facilities
- ☐ Disaster recovery for networks
- ☐ Diverse processing
- ☐ Disaster recovery for systems

Question 472

There are several types of penetration tests depending upon the scope, objective and nature of a test. Which of the following describes a penetration test where you attack and attempt to circumvent the controls of the targeted network from the outside, usually the Internet?

- ☐ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing

Question 473

An organization having a number of offices across a wide geographical area has developed a disaster recovery plan (DRP). Using actual resources, which of the following is the MOST cost-effective test of the DRP?

- ☐ Full operational test
- ☐ Preparedness test
- ☐ Paper test
- ☐ Regression test

Question 474

Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

- ☐ A substantive test of program library controls
- ☐ A compliance test of program library controls
- ☐ A compliance test of the program compiler controls
- ☐ A substantive test of the program compiler controls

Question 475

Which of the following ACID property ensures that transaction will bring the database from one valid state to another?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 476

An investment advisor e-mails periodic newsletters to clients and wants reasonable assurance that no one has modified the newsletter. This objective can be achieved by:

- ☐ encrypting the hash of the newsletter using the advisor's private key.
- ☐ encrypting the hash of the newsletter using the advisor's public key.
- ☐ digitally signing the document using the advisor's private key.
- ☐ encrypting the newsletter using the advisor's private key.

Question 477

Which of the following term related to network performance refers to the maximum rate that information can be transferred over a network?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 478

Which of the following is a data validation edit and control?

- ☐ Hash totals
- ☐ Reasonableness checks
- ☐ Online access controls
- ☐ Before and after image reporting

Question 479

Which of the following data validation control validates input data against predefined range values?

- ☐ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Question 480

Identify the INCORRECT statement related to network performance below?

- ☐ Bandwidth - Bandwidth commonly measured in bits/second is the maximum rate that information can be transferred
- ☐ Latency - Latency the actual rate that information is transferred
- ☐ Jitter - Jitter variation in the time of arrival at the receiver of the information
- ☐ Error Rate - Error rate the number of corrupted bits expressed as a percentage or fraction of the total sent

Question 481

Which of the following should be a concern to an IS auditor reviewing a wireless network?

- ☐ 128-bit static-key WEP (Wired Equivalent Privacy) encryption is enabled.
- ☐ SSID (Service Set Identifier) broadcasting has been enabled.
- ☐ Antivirus software has been installed in all wireless clients.
- ☐ MAC (Media Access Control) access control filtering has been deployed.

Question 482

Many organizations require an employee to take a mandatory vacation (holiday) of a week or more to:

- ☐ ensure the employee maintains a good quality of life, which will lead to greater productivity.
- ☐ reduce the opportunity for an employee to commit an improper or illegal act.
- ☐ provide proper cross-training for another employee.
- ☐ eliminate the potential disruption caused when an employee takes vacation one day at a time.

Question 483

Which of the following protocol is PRIMARILY used to provide confidentiality in a web based application thus protecting data sent across a client machine and a server?

- ☐ SSL
- ☐ FTP
- ☐ SSH
- ☐ S/MIME

Question 484

The PRIMARY purpose for meeting with auditees prior to formally closing a review is to:

- ☐ confirm that the auditors did not overlook any important issues.
- ☐ gain agreement on the findings.
- ☐ receive feedback on the adequacy of the audit procedures.
- ☐ test the structure of the final presentation.

Question 485

When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

- ☐ Business continuity self-audit
- ☐ Resource recovery analysis
- ☐ Risk assessment
- ☐ Gap analysis

Question 486

The MAJOR advantage of a component-based development approach is the:

- ☐ ability to manage an unrestricted variety of data types.
- ☐ provision for modeling complex relationships.
- ☐ capacity to meet the demands of a changing environment.
- ☐ support of multiple development environments.

Question 487

When reviewing a project where quality is a major concern, an IS auditor should use the project management triangle to explain that:

- ☐ increases in quality can be achieved, even if resource allocation is decreased.
- ☐ increases in quality are only achieved if resource allocation is increased.
- ☐ decreases in delivery time can be achieved, even if resource allocation is decreased.
- ☐ decreases in delivery time can only be achieved if quality is decreased.

Question 488

The quality of the metadata produced from a data warehouse is _____ in the warehouse's design.

- ☐ Often hard to determine because the data is derived from a heterogeneous data environment
- ☐ The most important consideration
- ☐ Independent of the quality of the warehoused databases
- ☐ Of secondary importance to data warehouse content

Question 489

Which of the following attack involves sending forged ICMP Echo Request packets to the broadcast address on multiple gateways in order to illicit responses from the computers behind the gateway where they all respond back with ICMP Echo Reply packets to the source IP address of the ICMP Echo Request packets?

- ☐ Reflected attack
- ☐ Brute force attack
- ☐ Buffer overflow
- ☐ Pulsing Zombie

Question 490

Which of the following should be included in an organization's IS security policy?

- ☐ A list of key IT resources to be secured
- ☐ The basis for access authorization
- ☐ Identity of sensitive security features
- ☐ Relevant software security features

Question 491

What type of risk is associated with authorized program exits (trap doors)?

- ☐ Business risk
- ☐ Audit risk
- ☐ Detective risk
- ☐ Inherent risk

Question 492

When preparing an audit report, the IS auditor should ensure that the results are supported by:

- ☐ statements from IS management.
- ☐ workpapers of other auditors.
- ☐ an organizational control self-assessment.
- ☐ sufficient and appropriate audit evidence.

Question 493

What is often the most difficult part of initial efforts in application development?

- ☐ Configuring software
- ☐ Planning security
- ☐ Determining time and resource requirements
- ☐ Configuring hardware

Question 494

Which of the following should an IS auditor use to detect duplicate invoice records within an invoice master file?

- ☐ Attribute sampling
- ☐ Generalized audit software (GAS)
- ☐ Test data
- ☐ Integrated test facility (ITF)

Question 495

When performing an IS strategy audit, an IS auditor should review both short-term (one- year) and long-term (three-to five-year) IS strategies, interview appropriate corporate management personnel, and ensure that the external environment has been considered. The auditor should especially focus on procedures in an audit of IS strategy. True or false?

- ☐ True
- ☐ False

Question 496

An IS auditor evaluates the test results of a modification to a system that deals with payment computation. The auditor finds that 50 percent of the calculations do not match predetermined totals. Which of the following would MOST likely be the next step in the audit?

- ☐ Design further tests of the calculations that are in error.
- ☐ Identify variables that may have caused the test results to be inaccurate.
- ☐ Examine some of the test cases to confirm the results.
- ☐ Document the results and prepare a report of findings, conclusions and recommendations.

Question 497

Which of the following statement is NOT true about Voice-Over IP (VoIP)?

VoIP uses circuit switching technology

Lower cost per call or even free calls, especially for long distance call

Lower infrastructure cost

VoIP is a technology where voice traffic is carried on top of existing data infrastructure

- ☐ VoIP uses circuit switching technology
- ☐ Lower cost per call or even free calls, especially for long distance call
- ☐ Lower infrastructure cost
- ☐ VoIP is a technology where voice traffic is carried on top of existing data infrastructure

Question 498

Human error is being HEAVILY relied upon on by which of the following types of attack?

- ☐ Eavedropping
- ☐ DoS
- ☐ DDoS
- ☐ ATP
- ☐ Social Engineering
- ☐ None of the choices.

Question 499

During an implementation review of a multiuser distributed application, an IS auditor finds minor weaknesses in three areas-the initial setting of parameters is improperly installed, weak passwords are being used and some vital reports are not being checked properly. While preparing the audit report, the IS auditor should:

- ☐ record the observations separately with the impact of each of them marked against each respective finding.
- ☐ advise the manager of probable risks without recording the observations, as the control weaknesses are minor ones.
- ☐ record the observations and the risk arising from the collective weaknesses.
- ☐ apprise the departmental heads concerned with each observation and properly document it in the report.

Question 500

Identify the correct sequence of Business Process Reengineering (BPR) benchmarking process from the given choices below?

- ☐ PLAN, RESEARCH, OBSERVE, ANALYZE, ADOPT and IMPROVE
- ☐ OBSERVE, PLAN, RESEACH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, OBSERVE, RESEARCH, ANALYZE, ADOPT and IMPROVE
- ☐ PLAN, RESEARCH, ANALYZE, OBSERVE, ADOPT and IMPROVE

Question 501

Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?

- ☐ Circuit gateway
- ☐ Application gateway
- ☐ Packet filter
- ☐ Screening router

Question 502

Which of the following should be included in a feasibility study for a project to implement an EDI process?

- ☐ The encryption algorithm format
- ☐ The detailed internal control procedures
- ☐ The necessary communication protocols
- ☐ The proposed trusted third-party agreement

Question 503

Which of the following data validation edits is effective in detecting transposition and transcription errors?

- ☐ Range check
- ☐ Check digit
- ☐ Validity check
- ☐ Duplicate check

Question 504

Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?

- ☐ Paper test
- ☐ Post test
- ☐ Preparedness test
- ☐ Walk-through

Question 505

By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:

- ☐ reliable products are guaranteed.
- ☐ programmers' efficiency is improved.
- ☐ security requirements are designed.
- ☐ predictable software processes are followed.

Question 506

Which of the following BEST describes the necessary documentation for an enterprise product reengineering (EPR) software installation?

- ☐ Specific developments only
- ☐ Business requirements only
- ☐ All phases of the installation must be documented
- ☐ No need to develop a customer specific documentation

Question 507

When reviewing the configuration of network devices, an IS auditor should FIRST identify:

- ☐ the best practices for the type of network devices deployed.
- ☐ whether components of the network are missing.
- ☐ the importance of the network device in the topology.
- ☐ whether subcomponents of the network are being used appropriately.

Question 508

Which of the following layer of an enterprise data flow architecture represents subset of information from the core Data Warehouse selected and organized to meet the needs of a particular business unit or business line?

- ☐ Data preparation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 509

Which of the following is the MOST important objective of data protection?

- ☐ identifying persons who need access to information
- ☐ Ensuring the integrity of information
- ☐ Denying or authorizing access to the IS system
- ☐ Monitoring logical accesses

Question 510

The rate of change in technology increases the importance of:

- ☐ outsourcing the IS function.
- ☐ implementing and enforcing good processes.
- ☐ hiring personnel willing to make a career within the organization.
- ☐ meeting user requirements.

Question 511

During which of the following phases in system development would user acceptance test plans normally be prepared?

- ☐ Feasibility study
- ☐ Requirements definition
- ☐ implementation planning
- ☐ Postimplementation review

Question 512

A sequence of bits appended to a digital document that is used to secure an e-mail sent through the Internet is called a:

- ☐ digest signature.
- ☐ electronic signature.
- ☐ digital signature.
- ☐ hash signature.

Question 513

An IS auditor reviewing the implementation of an intrusion detection system (IDS) should be MOST concerned if:

- ☐ IDS sensors are placed outside of the firewall.
- ☐ a behavior-based IDS is causing many false alarms.
- ☐ a signature-based IDS is weak against new types of attacks.
- ☐ the IDS is used to detect encrypted traffic.

Question 514

Which of the following is a ITU-T standard protocol suite for packet switched wide area network communication?

- ☐ Point-to-point protocol
- ☐ X.25
- ☐ Frame Relay
- ☐ ISDN

Question 515

Machines that operate as a closed system can NEVER be eavesdropped.

- ☐ True
- ☐ False

Question 516

The PRIMARY reason an IS auditor performs a functional walkthrough during the preliminary phase of an audit assignment is to:

- ☐ understand the business process.
- ☐ comply with auditing standards.
- ☐ identify control weakness.
- ☐ plan substantive testing.

Question 517

To properly evaluate the collective effect of preventative, detective, or corrective controls within a process, an IS auditor should be aware of which of the following?

- ☐ The business objectives of the organization
- ☐ The effect of segregation of duties on internal controls
- ☐ The point at which controls are exercised as data flows through the system
- ☐ Organizational control policies

Question 518

To develop a successful business continuity plan, end user involvement is critical during which of the following phases?

- ☐ Business recovery strategy
- ☐ Detailed plan development
- ☐ Business impact analysis (BIA)
- ☐ Testing and maintenance

Question 519

Which of the following biometrics methods provides the HIGHEST accuracy and is LEAST accepted by users?

- ☐ Palm Scan
- ☐ Hand Geometry
- ☐ Fingerprint
- ☐ Retina scan

Question 520

Everything not explicitly permitted is forbidden has which of the following kinds of tradeoff?

- ☐ it improves security at a cost in functionality.
- ☐ it improves functionality at a cost in security.
- ☐ it improves security at a cost in system performance.
- ☐ it improves performance at a cost in functionality.
- ☐ None of the choices.

Question 521

Which of the following would impair the independence of a quality assurance team?

- ☐ Ensuring compliance with development methods
- ☐ Checking the testing assumptions
- ☐ Correcting coding errors during the testing process
- ☐ Checking the code to ensure proper documentation

Question 522

From a control perspective, the key element in job descriptions is that they:

- ☐ provide instructions on how to do the job and define authority.
- ☐ are current, documented and readily available to the employee.
- ☐ communicate management's specific job performance expectations.
- ☐ establish responsibility and accountability for the employee's actions.

Question 523

An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:

- ☐ fast synthetic backups for offsite storage are supported.
- ☐ backup to disk is always significantly faster than backup to tape.
- ☐ tape libraries are no longer needed.
- ☐ data storage on disks is more reliable than on tapes.

Question 524

An IS auditor conducting a review of software usage and licensing discovers that numerous PCs contain unauthorized software. Which of the following actions should the IS auditor take?

- ☐ Personally delete all copies of the unauthorized software.
- ☐ Inform the auditee of the unauthorized software, and follow up to confirm deletion.
- ☐ Report the use of the unauthorized software and the need to prevent recurrence to auditee management.
- ☐ Take no action, as it is a commonly accepted practice and operations management is responsible for monitoring such use.

Question 525

Which of the following software development methods is based on iterative and incremental development, where requirements and solutions evolve through collaboration between self-organizing, cross-functional teams?

- ☐ Agile Development
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 526

Which of the following potentially blocks hacking attempts?

- ☐ intrusion detection system
- ☐ Honeypot system
- ☐ Intrusion prevention system
- ☐ Network security scanner

Question 527

Which of the following is the MOST critical step in planning an audit?

- ☐ Implementing a prescribed auditing framework such as COBIT
- ☐ Identifying current controls
- ☐ Identifying high-risk audit targets
- ☐ Testing controls

Question 528

When reviewing an intrusion detection system (IDS), an IS auditor should be MOST concerned about which of the following?

- ☐ Number of nonthreatening events identified as threatening
- ☐ Attacks not being identified by the system
- ☐ Reports/logs being produced by an automated tool
- ☐ Legitimate traffic being blocked by the system

Question 529

What is a callback system?

- ☐ It is a remote-access system whereby the remote-access server immediately calls the user back at a predetermined number if the dial-in connection fails.
- ☐ It is a remote-access system whereby the user's application automatically redials the remote access server if the initial connection attempt fails.
- ☐ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently dials the user back at a predetermined number stored in the server's configuration database.
- ☐ It is a remote-access control whereby the user initially connects to the network systems via dial-up access, only to have the initial connection terminated by the server, which then subsequently allows the user to call back at an approved number for a limited period of time.

Question 530

Within IPSEC which of the following defines security parameters which should be applied between communicating parties such as encryption algorithms, key initialization vector, life span of keys, etc?

- ☐ Security Parameter Index (SPI)
- ☐ Security Association (SA)
- ☐ Encapsulation Security Payload (ESP)
- ☐ Authentication Header (AH)

Question 531

Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- ☐ Review the parameter settings.
- ☐ Interview the firewall administrator.
- ☐ Review the actual procedures.
- ☐ Review the device's log file for recent attacks.

Question 532

Which of the following line media would provide the BEST security for a telecommunication network?

- ☐ broadband network digital transmission
- ☐ Baseband network
- ☐ Dial-up
- ☐ Dedicated lines

Question 533

An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

- ☐ Recommend that an additional comprehensive BCP be developed.
- ☐ Determine whether the BCPs are consistent.
- ☐ Accept the BCPs as written.
- ☐ Recommend the creation of a single BCP.

Question 534

An IS auditor examining the configuration of an operating system to verify the controls should review the:

- ☐ transaction logs.
- ☐ authorization tables.
- ☐ parameter settings.
- ☐ routing tables.

Question 535

Which of the following is protocol data unit (PDU) of network interface layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 536

An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- ☐ the setup is geographically dispersed.
- ☐ the network servers are clustered in a site.
- ☐ a hot site is ready for activation.
- ☐ diverse routing is implemented for the network.

Question 537

Which of the following ACID property in DBMS means that once a transaction has been committed, it will remain so, even in the event of power loss, crashes, or errors?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 538

The GREATEST benefit in implementing an expert system is the:

- ☐ capturing of the knowledge and experience of individuals in an organization.
- ☐ sharing of knowledge in a central repository.
- ☐ enhancement of personnel productivity and performance.
- ☐ reduction of employee turnover in key departments.

Question 539

Risk analysis is not always possible because the IS auditor is attempting to calculate risk using nonquantifiable threats and potential losses. In this event, a _____ risk assessment is more appropriate. Fill in the blanks.

- ☐ Quantitative; qualitative
- ☐ Qualitative; quantitative
- ☐ Residual; subjective
- ☐ Quantitative; subjective

Question 540

Which of the following public key infrastructure (PKI) elements provides detailed descriptions for dealing with a compromised private key?

- ☐ Certificate revocation list (CRL)
- ☐ Certification practice statement (CPS)
- ☐ Certificate policy (CP)
- ☐ PKI disclosure statement (PDS)

Question 541

An advantage of using sanitized live transactions in test data is that:

- ☐ all transaction types will be included.
- ☐ every error condition is likely to be tested.
- ☐ no special routines are required to assess the results.
- ☐ test transactions are representative of live processing.

Question 542

In the course of performing a risk analysis, an IS auditor has identified threats and potential impacts. Next, the IS auditor should:

- ☐ identify and assess the risk assessment process used by management.
- ☐ identify information assets and the underlying systems.
- ☐ disclose the threats and impacts to management.
- ☐ identify and evaluate the existing controls.

Question 543

Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

- ☐ Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
- ☐ During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
- ☐ The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
- ☐ Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Question 544

With the objective of mitigating the risk and impact of a major business interruption, a disaster recovery plan should endeavor to reduce the length of recovery time necessary, as well as costs associated with recovery. Although DRP results in an increase of pre-and post-incident operational costs, the extra costs are more than offset by reduced recovery and business impact costs. True or false?

- ☐ True
- ☐ False

Question 545

An organization has outsourced its wide area network (WAN) to a third-party service provider. Under these circumstances, which of the following is the PRIMARY task the IS auditor should perform during an audit of business continuity (BCP) and disaster recovery planning (DRP)?

- ☐ Review whether the service provider's BCP process is aligned with the organization's BCP and contractual obligations.
- ☐ Review whether the service level agreement (SLA) contains a penalty clause in case of failure to meet the level of service in case of a disaster.
- ☐ Review the methodology adopted by the organization in choosing the service provider.
- ☐ Review the accreditation of the third-party service provider's staff.

Question 546

Run-to-run totals can verify data through which stage(s) of application processing?

- ☐ Initial
- ☐ Various
- ☐ Final
- ☐ Output

Question 547

Which of the following is the PRIMARY advantage of using computer forensic software for investigations?

- ☐ The preservation of the chain of custody for electronic evidence
- ☐ Time and cost savings
- ☐ Efficiency and effectiveness
- ☐ Ability to search for violations of intellectual property rights

Question 548

Buffer overflow aims primarily at corrupting:

- ☐ system processor
- ☐ network firewall
- ☐ system memory
- ☐ disk storage
- ☐ None of the choices.

Question 549

The knowledge base of an expert system that uses questionnaires to lead the user through a series of choices before a conclusion is reached is known as:

- ☐ rules.
- ☐ decision trees.
- ☐ semantic nets.
- ☐ dataflow diagrams.

Question 550

ALL computer programming languages are vulnerable to command injection attack.

- ☐ True
- ☐ False

Question 551

Upon receipt of the initial signed digital certificate the user will decrypt the certificate with the public key of the:

- ☐ registration authority (RA).
- ☐ certificate authority (CA).
- ☐ certificate repository.
- ☐ receiver.

Question 552

Which of the following provides the MOST relevant information for proactively strengthening security settings?

- ☐ Bastion host
- ☐ Intrusion detection system
- ☐ Honeypot
- ☐ Intrusion prevention system

Question 553

Although BCP and DRP are often implemented and tested by middle management and end users, the ultimate responsibility and accountability for the plans remain with executive management, such as the _____. (fill-in-the-blank)

- ☐ Security administrator
- ☐ Systems auditor
- ☐ Board of directors
- ☐ Financial auditor

Question 554

Which of the following term related to network performance refers to the variation in the time of arrival of packets on the receiver of the information?

- ☐ Bandwidth
- ☐ Throughput
- ☐ Latency
- ☐ Jitter

Question 555

Which of the following statement INCORRECTLY describes anti-malware?

- ☐ 2
- ☐ 3
- ☐ 2 and 3
- ☐ None of the choices listed

Question 556

Which of the following terms is used more generally for describing concealment routines in a malicious program?

- ☐ virus
- ☐ worm
- ☐ trojan horse
- ☐ spyware
- ☐ rootkits
- ☐ backdoor
- ☐ None of the choices.

Question 557

Which of the following is best suited for searching for address field duplications?

- ☐ Text search forensic utility software
- ☐ Generalized audit software
- ☐ Productivity audit software
- ☐ Manual review

Question 558

Which of the following term in business continuity defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 559

An IS auditor is evaluating a corporate network for a possible penetration by employees. Which of the following findings should give the IS auditor the GREATEST concern?

- ☐ There are a number of external modems connected to the network.
- ☐ Users can install software on their desktops.
- ☐ Network monitoring is very limited.
- ☐ Many user IDs have identical passwords.

Question 560

A comprehensive and effective e-mail policy should address the issues of e-mail structure, policy enforcement, monitoring and:

- ☐ recovery.
- ☐ retention.
- ☐ rebuilding.
- ☐ reuse.

Question 561

What process allows IS management to determine whether the activities of the organization differ from the planned or expected levels?

- ☐ Business impact assessment
- ☐ Risk assessment
- ☐ IS assessment methods
- ☐ Key performance indicators (KPIs)

Question 562

Which of the following forms of evidence for the auditor would be considered the MOST reliable?

- ☐ An oral statement from the auditee
- ☐ The results of a test performed by an IS auditor
- ☐ An internally generated computer accounting report
- ☐ A confirmation letter received from an outside source

Question 563

The PRIMARY advantage of a continuous audit approach is that it:

- ☐ does not require an IS auditor to collect evidence on system reliability while processing is taking place.
- ☐ requires the IS auditor to review and follow up immediately on all information collected.
- ☐ can improve system security when used in time-sharing environments that process a large number of transactions.
- ☐ does not depend on the complexity of an organization's computer systems.

Question 564

An IS auditor is assigned to perform a post implementation review of an application system. Which of the following situations may have impaired the independence of the IS auditor? The IS auditor:

- ☐ implemented a specific control during the development of the application system.
- ☐ designed an embedded audit module exclusively for auditing the application system.
- ☐ participated as a member of the application system project team, but did not have operational responsibilities.
- ☐ provided consulting advice concerning application system best practices.

Question 565

Which of the following are effective controls for detecting duplicate transactions such as payments made or received?

- ☐ Concurrency controls
- ☐ Reasonableness checks
- ☐ Time stamps
- ☐ Referential integrity controls

Question 566

_____ (fill in the blank) is/are ultimately accountable for the functionality, reliability, and security within IT governance.

- ☐ Data custodians
- ☐ The board of directors and executive officers
- ☐ IT security administration
- ☐ Business unit managers

Question 567

Which of the following is a control over component communication failure/errors?

- ☐ Restricting operator access and maintaining audit trails
- ☐ Monitoring and reviewing system engineering activity
- ☐ Providing network redundancy
- ☐ Establishing physical barriers to the data transmitted over the network

Question 568

Which of the following is the process of repeating a portion of a test scenario or test plan to ensure that changes in information system have not introduced any errors?

- ☐ Parallel Test
- ☐ Black box testing
- ☐ Regression Testing
- ☐ Pilot Testing

Question 569

The vice president of human resources has requested an audit to identify payroll overpayments for the previous year. Which would be the BEST audit technique to use in this situation?

- ☐ Test data
- ☐ Generalized audit software
- ☐ Integrated test facility
- ☐ Embedded audit module

Question 570

Distributed denial-of-service (DDOS) attacks on Internet sites are typically evoked by hackers using which of the following?

- ☐ Logic bombs
- ☐ Phishing
- ☐ Spyware
- ☐ Trojan horses

Question 571

Which of the following layer of an enterprise data flow architecture represents subsets of information from the core data warehouse?

- ☐ Presentation layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 572

Which of the following IT governance best practices improves strategic alignment?

- ☐ Supplier and partner risks are managed.
- ☐ A knowledge base on customers, products, markets and processes is in place.
- ☐ A structure is provided that facilitates the creation and sharing of business information.
- ☐ Top management mediate between the imperatives of business and technology.

Question 573

What is the primary objective of a control self-assessment (CSA) program?

- ☐ Enhancement of the audit responsibility
- ☐ Elimination of the audit responsibility
- ☐ Replacement of the audit responsibility
- ☐ Integrity of the audit responsibility

Question 574

An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- ☐ A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- ☐ Firewall policies are updated on the basis of changing requirements.
- ☐ inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- ☐ The firewall is placed on top of the commercial operating system with all installation options.

Question 575

Which of the following types of attack makes use of unfiltered user input as the format string parameter in the print () function of the C language?

- ☐ buffer overflows
- ☐ format string vulnerabilities
- ☐ integer overflow
- ☐ code injection
- ☐ command injection
- ☐ None of the choices.

Question 576

Which of the following help(s) prevent an organization's systems from participating in a distributed denial-of-service (DDoS) attack?

- ☐ Inbound traffic filtering
- ☐ Using access control lists (ACLs) to restrict inbound connection attempts
- ☐ Outbound traffic filtering
- ☐ Recentralizing distributed systems

Question 577

Which of the following malware technical fool's malware by appending section of themselves to files – somewhat in the same way that file malware append themselves?

- ☐ Scanners
- ☐ Active Monitors
- ☐ Immunizer
- ☐ Behavior blocker

Question 578

Which of the following term in business continuity determines the maximum acceptable amount of data loss measured in time?

- ☐ RPO
- ☐ RTO
- ☐ WRT
- ☐ MTD

Question 579

Which of the following control make sure that input data comply with predefined criteria maintained in computerized table of possible values?

- ☐ Range Check
- ☐ Table lookups
- ☐ Existence check
- ☐ Reasonableness check

Question 580

Hamid needs to shift users from using the application from the existing (Old) system to the replacing (new) system. His manager Lily has suggested he uses an approach in which the newer system is changed over from the older system on a cutoff date and time and the older system is discontinued once the changeover to the new system takes place. Which of the following changeover approach is suggested by Lily?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☐ Abrupt changeover
- ☐ Pilot changeover

Question 581

The directory system of a database-management system describes:

- ☐ The access method to the data
- ☐ The location of data AND the access method
- ☐ The location of data
- ☐ Neither the location of data NOR the access method

Question 582

In the context of effective information security governance, the primary objective of value delivery is to:

- ☐ optimize security investments in support of business objectives.
- ☐ implement a standard set of security practices.
- ☐ institute a standards-based solution.
- ☐ implement a continuous improvement culture.

Question 583

In transport mode, the use of the Encapsulating Security Payload (ESP) protocol is advantageous over the Authentication Header (AH) protocol because it provides:

- ☐ connectionless integrity.
- ☐ data origin authentication.
- ☐ antireplay service.
- ☐ confidentiality.

Question 584

Which of the following environmental controls is appropriate to protect computer equipment against short-term reductions in electrical power?

- ☐ Power line conditioners
- ☐ Surge protective devices
- ☐ Alternative power supplies
- ☐ Interruptible power supplies

Question 585

An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?

- ☐ Pilot
- ☐ Parallel
- ☐ Direct cutover
- ☐ Phased

Question 586

Who is responsible for providing adequate physical and logical security for IS program, data and equipment?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 587

The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- ☐ use this information to launch attacks.
- ☐ forward the security alert.
- ☐ implement individual solutions.
- ☐ fail to understand the threat.

Question 588

Which of the following refers to the proving of mathematical theorems by a computer program?

- ☐ Analytical theorem proving
- ☐ Automated technology proving
- ☐ Automated theorem processing
- ☐ Automated theorem proving
- ☐ None of the choices.

Question 589

An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?

- ☐ Consider feasibility of a separate user acceptance environment
- ☐ Schedule user testing to occur at a given time each day
- ☐ implement a source code version control tool
- ☐ Only retest high priority defects

Question 590

Which of the following is BEST characterized by unauthorized modification of data before or during systems data entry?

- ☐ Data diddling
- ☐ Skimming
- ☐ Data corruption
- ☐ Salami attack

Question 591

Which of the following would prevent accountability for an action performed, thus allowing nonrepudiation?

- ☐ Proper authentication
- ☐ Proper identification AND authentication
- ☐ Proper identification
- ☐ Proper identification, authentication, AND authorization

Question 592

While evaluating logical access control the IS auditor should follow all of the steps mentioned below EXCEPT one?

1. Obtain general understanding of security risk facing information processing, through a review of relevant documentation, inquiry and observation, etc
2. Document and evaluate controls over potential access paths into the system to assess their adequacy, efficiency and effectiveness
3. Test Control over access paths to determine whether they are functioning and effective by applying appropriate audit technique
4. Evaluate the access control environment to determine if the control objective are achieved by analyzing test result and other audit evidence
5. Evaluate the security environment to assess its adequacy by reviewing written policies, observing practices and procedures, and comparing them with appropriate security standard or practice and procedures used by other organization.
6. Evaluate and deploy technical controls to mitigate all identified risks during audit.

- ☐ 2
- ☐ 3
- ☐ 1
- ☐ 6

Question 593

Which of the following layer of an enterprise data flow architecture is responsible for data copying, transformation in Data Warehouse (DW) format and quality control?

- ☐ Data Staging and quality layer
- ☐ Desktop Access Layer
- ☐ Data Mart layer
- ☐ Data access layer

Question 594

The MOST likely effect of the lack of senior management commitment to IT strategic planning is:

- ☐ a lack of investment in technology.
- ☐ a lack of a methodology for systems development.
- ☐ technology not aligning with the organization's objectives.
- ☐ an absence of control over technology contracts.

Question 595

A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not adequately performing which of the following types of testing?

- ☐ Unit testing
- ☐ Integration testing
- ☐ Design walk-throughs
- ☐ Configuration management

Question 596

An example of a direct benefit to be derived from a proposed IT-related business investment is:

- ☐ enhanced reputation.
- ☐ enhanced staff morale.
- ☐ the use of new technology.
- ☐ increased market penetration.

Question 597

The advantage of a bottom-up approach to the development of organizational policies is that the policies:

- ☐ are developed for the organization as a whole
- ☐ are more likely to be derived as a result of a risk assessment.
- ☐ will not conflict with overall corporate policy.
- ☐ ensure consistency across the organization.

Question 598

Which of the following network configuration options contains a direct link between any two host machines?

- ☐ Bus
- ☐ Ring
- ☐ Star
- ☐ Completely connected (mesh)

Question 599

What is an effective countermeasure for the vulnerability of data entry operators potentially leaving their computers without logging off?

- ☐ Employee security awareness training
- ☐ Administrator alerts
- ☐ Screensaver passwords
- ☐ Close supervision

Question 600

Which of the following is MOST critical during the business impact assessment phase of business continuity planning?

- ☐ End-user involvement
- ☐ Senior management involvement
- ☐ Security administration involvement
- ☐ IS auditing involvement

Question 601

Which of the following software development methodology is a reuse-based approach to defining, implementing and composing loosely coupled independent components into systems?

- ☐ Agile Developments
- ☐ Software prototyping
- ☐ Rapid application development
- ☐ Component based development

Question 602

When developing a risk-based audit strategy, an IS auditor conduct a risk assessment to ensure that:

- ☐ controls needed to mitigate risks are in place.
- ☐ vulnerabilities and threats are identified.
- ☐ audit risks are considered.
- ☐ a gap analysis is appropriate.

Question 603

Which of the following is a standard secure email protection protocol?

- ☐ S/MIME
- ☐ SSH
- ☐ SET
- ☐ S/HTTP

Question 604

Introducing inhomogeneity to your network for the sake of robustness would have which of the following drawbacks?

- ☐ poorer performance.
- ☐ poor scalability.
- ☐ weak infrastructure.
- ☐ high costs in terms of training and maintenance.
- ☐ None of the choices.

Question 605

A top-down approach to the development of operational policies will help ensure:

- ☐ that they are consistent across the organization.
- ☐ that they are implemented as a part of risk assessment.
- ☐ compliance with all policies.
- ☐ that they are reviewed periodically.

Question 606

Which of the following statement INCORRECTLY describes circuit switching technique?

- ☐ Packet uses many different dynamic paths to get the same destination
- ☐ Connection oriented virtual links
- ☐ Fixed delays
- ☐ Traffic travels in a predictable and constant manner

Question 607

When implementing an IT governance framework in an organization the MOST important objective is:

- ☐ IT alignment with the business.
- ☐ accountability.
- ☐ value realization with IT.
- ☐ enhancing the return on IT investments.

Question 608

Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?

- ☐ A user from within could send a file to an unauthorized person.
- ☐ FTP services could allow a user to download files from unauthorized sources.
- ☐ A hacker may be able to use the FTP service to bypass the firewall.
- ☐ FTP could significantly reduce the performance of a DMZ server.

Question 609

The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- ☐ make unauthorized changes to the database directly, without an audit trail.
- ☐ make use of a system query language (SQL) to access information.
- ☐ remotely access the database.
- ☐ update data without authentication.

Question 610

What can ISPs use to implement inbound traffic filtering as a control to identify IP packets transmitted from unauthorized sources?

- ☐ OSI Layer 2 switches with packet filtering enabled
- ☐ Virtual Private Networks
- ☐ Access Control Lists (ACL)
- ☐ Point-to-Point Tunneling Protocol

Question 611

After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?

- ☐ Differential reporting
- ☐ False-positive reporting
- ☐ False-negative reporting
- ☐ Less-detail reporting

Question 612

The traditional role of an IS auditor in a control self-assessment (CSA) should be that of a(n):

- ☐ Implementor
- ☐ Facilitator
- ☐ Developer
- ☐ Sponsor

Question 613

To assist an organization in planning for IT investments, an IS auditor should recommend the use of:

- ☐ project management tools.
- ☐ an object-oriented architecture.
- ☐ tactical planning.
- ☐ enterprise architecture (EA).

Question 614

Confidentiality of the data transmitted in a wireless LAN is BEST protected if the session is:

- ☐ restricted to predefined MAC addresses.
- ☐ encrypted using static keys.
- ☐ encrypted using dynamic keys.
- ☐ initiated from devices that have encrypted storage.

Question 615

Two-factor authentication can be circumvented through which of the following attacks?

- ☐ Denial-of-service
- ☐ Man-in-the-middle
- ☐ Key logging
- ☐ Brute force

Question 616

An IS auditor should know information about different network transmission media. Which of the following transmission media is used for short distance transmission?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Satellite Radio Link

Question 617

Which type of major BCP test only requires representatives from each operational area to meet to review the plan?

- ☐ Parallel
- ☐ Preparedness
- ☐ Walk-thorough
- ☐ Paper

Question 618

An organization's IS audit charter should specify the:

- ☐ short- and long-term plans for IS audit engagements
- ☐ objectives and scope of IS audit engagements.
- ☐ detailed training plan for the IS audit staff.
- ☐ role of the IS audit function.

Question 619

Network environments often add to the complexity of program-to-program communication, making the implementation and maintenance of application systems more difficult. True or false?

- ☐ True
- ☐ False

Question 620

When a new system is to be implemented within a short time frame, it is MOST important to:

- ☐ finish writing user manuals.
- ☐ perform user acceptance testing.
- ☐ add last-minute enhancements to functionalities.
- ☐ ensure that the code has been documented and reviewed.

Question 621

A LAN administrator normally would be restricted from:

- ☐ having end-user responsibilities.
- ☐ reporting to the end-user manager.
- ☐ having programming responsibilities.
- ☐ being responsible for LAN security administration.

Question 622

An integrated test facility is not considered a useful audit tool because it cannot compare processing output with independently calculated data. True or false?

- ☐ True
- ☐ False

Question 623

The PRIMARY objective of performing a postincident review is that it presents an opportunity to:

- ☐ improve internal control procedures.
- ☐ harden the network to industry best practices.
- ☐ highlight the importance of incident response management to management.
- ☐ improve employee awareness of the incident response process.

Question 624

Which of the following transmission media is LEAST vulnerable to cross talk?

- ☐ Copper cable
- ☐ Fiber Optics
- ☐ Satellite Radio Link
- ☐ Coaxial cable

Question 625

The information in the knowledge base can be expressed in several ways. Which of the following way uses questionnaires to lead the user through a series of choices until a conclusion is reached?

- ☐ Decision tree
- ☐ Rules
- ☐ Semantic nets
- ☐ Knowledge interface

Question 626

Which of the following statement INCORRECTLY describes packet switching technique?

- ☐ Packet uses many different dynamic paths to get the same destination
- ☐ Traffic is usually burst in nature
- ☐ Fixed delays to reach each packet to destination
- ☐ Usually carries data-oriented data

Question 627

When installing an intrusion detection system (IDS), which of the following is MOST important?

- ☐ Properly locating it in the network architecture
- ☐ Preventing denial-of-service (DoS) attacks
- ☐ Identifying messages that need to be quarantined
- ☐ Minimizing the rejection errors

Question 628

Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

- ☐ a firewall exists.
- ☐ a secure web connection is used.
- ☐ the source of the executable file is certain.
- ☐ the host web site is part of the organization.

Question 629

William has been assigned a changeover task. He has to break the older system into deliverable modules. Initially, the first module of the older system is phased out using the first module of a new system. Then, the second module of the old system is phased out, using the second module of the newer system and so forth until reaching the last module. Which of the following changeover system William needs to implement?

- ☐ Parallel changeover
- ☐ Phased changeover
- ☐ Abrupt changeover
- ☐ Pilot changeover

Question 630

Who is responsible for restricting and monitoring access of a data user?

- ☐ Data Owner
- ☐ Data User
- ☐ Data Custodian
- ☐ Security Administrator

Question 631

Which of the following is the GREATEST risk of an inadequate policy definition for ownership of data and systems?

- ☐ User management coordination does not exist.
- ☐ Specific user accountability cannot be established.
- ☐ Unauthorized users may have access to originate, modify or delete data.
- ☐ Audit recommendations may not be implemented.

Question 632

Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

- ☐ Filters
- ☐ Switches
- ☐ Routers
- ☐ Firewalls

Question 633

An intentional or unintentional disclosure of a password is likely to be evident within control logs.
True or false?

- ☐ True
- ☐ False

Question 634

Which of the following are designed to detect network attacks in progress and assist in post- attack forensics?

- ☐ Intrusion Detection Systems
- ☐ Audit trails
- ☐ System logs
- ☐ Tripwire
- ☐ None of the choices.

Question 635

Which of the following can degrade network performance?

- ☐ Superfluous use of redundant load-sharing gateways
- ☐ Increasing traffic collisions due to host congestion by creating new collision domains
- ☐ Inefficient and superfluous use of network devices such as switches
- ☐ Inefficient and superfluous use of network devices such as hubs

Question 636

A substantive test to verify that tape library inventory records are accurate is:

- ☐ determining whether bar code readers are installed.
- ☐ determining whether the movement of tapes is authorized.
- ☐ conducting a physical count of the tape inventory.
- ☐ checking if receipts and issues of tapes are accurately recorded.

Question 637

Which of the following protocol is used for electronic mail service?

- ☐ DNS
- ☐ FTP
- ☐ SSH
- ☐ SMTP

Question 638

Default permit is only a good approach in an environment where:

- ☐ security threats are non-existent or negligible.
- ☐ security threats are non-negligible.
- ☐ security threats are serious and severe.
- ☐ users are trained.
- ☐ None of the choices.

Question 639

Which of the following is BEST suited for secure communications within a small group?

- ☐ Key distribution center
- ☐ Certification authority
- ☐ Web of trust
- ☐ Kerberos Authentication System

Question 640

Overall business risk for a particular threat can be expressed as:

- ☐ a product of the probability and magnitude of the impact if a threat successfully exploits a vulnerability.
- ☐ the magnitude of the impact should a threat source successfully exploit the vulnerability.
- ☐ the likelihood of a given threat source exploiting a given vulnerability.
- ☐ the collective judgment of the risk assessment team.

Question 641

What is a reliable technique for estimating the scope and cost of a software-development project?

- ☐ Function point analysis (FPA)
- ☐ Feature point analysis (FPA)
- ☐ GANTT
- ☐ PERT

Question 642

An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:

- ☐ a data loss of up to 1 minute, but the processing must be continuous.
- ☐ a 1-minute processing interruption but cannot tolerate any data loss.
- ☐ a processing interruption of 1 minute or more.
- ☐ both a data loss and processing interruption longer than 1 minute.

Question 643

Which of the following should be of MOST concern to an IS auditor?

- ☐ Lack of reporting of a successful attack on the network
- ☐ Failure to notify police of an attempted intrusion
- ☐ Lack of periodic examination of access rights
- ☐ Lack of notification to the public of an intrusion

Question 644

Which of the following is an effective method for controlling downloading of files via FTP?

- ☐ An application-layer gateway, or proxy firewall, but not stateful inspection firewalls
- ☐ An application-layer gateway, or proxy firewall
- ☐ A circuit-level gateway
- ☐ A first-generation packet-filtering firewall

Question 645

Which of the following layer in an enterprise data flow architecture is directly death with by end user with information?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☐ Data mart layer
- ☐ Data access layer

Question 646

Which of the following process consist of identification and selection of data from the imaged data set in computer forensics?

- ☐ Investigation
- ☐ Interrogation
- ☐ Reporting
- ☐ Extraction

Question 647

Which of the following systems-based approaches would a financial processing company employ to monitor spending patterns to identify abnormal patterns and report them?

- ☐ A neural network
- ☐ Database management software
- ☐ Management information systems
- ☐ Computer assisted audit techniques

Question 648

An IS auditor should be MOST concerned with what aspect of an authorized honeypot?

- ☐ The data collected on attack methods
- ☐ The information offered to outsiders on the honeypot
- ☐ The risk that the honeypot could be used to launch further attacks on the organization's infrastructure
- ☐ The risk that the honeypot would be subject to a distributed denial-of-service attack

Question 649

To ensure an organization is complying with privacy requirements, an IS auditor should FIRST review:

- ☐ the IT infrastructure.
- ☐ organizational policies, standards and procedures.
- ☐ legal and regulatory requirements.
- ☐ the adherence to organizational policies, standards and procedures.

Question 650

The development of an IS security policy is ultimately the responsibility of the:

- ☐ IS department.
- ☐ security committee.
- ☐ security administrator.
- ☐ board of directors.

Question 651

Which of the following is a characteristic of timebox management?

- ☐ Not suitable for prototyping or rapid application development (RAD)
- ☐ Eliminates the need for a quality process
- ☐ Prevents cost overruns and delivery delays
- ☐ Separates system and user acceptance testing

Question 652

When an employee is terminated from service, the MOST important action is to:

- ☐ hand over all of the employee's files to another designated employee.
- ☐ complete a backup of the employee's work.
- ☐ notify other employees of the termination.
- ☐ disable the employee's logical access.

Question 653

An organization has a mix of access points that cannot be upgraded to stronger security and newer access points having advanced wireless security. An IS auditor recommends replacing the non-upgradeable access points. Which of the following would BEST justify the IS auditor's recommendation?

- ☐ The new access points with stronger security are affordable.
- ☐ The old access points are poorer in terms of performance.
- ☐ The organization's security would be as strong as its weakest points.
- ☐ The new access points are easier to manage.

Question 654

Which of the following type of lock uses a magnetic or embedded chip based plastic card key or token entered into a sensor/reader to gain access?

- ☐ Bolting door locks
- ☐ Combination door lock
- ☐ Electronic door lock
- ☐ Biometric door lock

Question 655

The purpose of a deadman door controlling access to a computer facility is primarily to:

- ☐ prevent piggybacking.
- ☐ prevent toxic gases from entering the data center.
- ☐ starve a fire of oxygen.
- ☐ prevent an excessively rapid entry to, or exit from, the facility.

Question 656

A web server is attacked and compromised. Which of the following should be performed FIRST to handle the incident?

- ☐ Dump the volatile storage data to a disk.
- ☐ Run the server in a fail-safe mode.
- ☐ Disconnect the web server from the network.
- ☐ Shut down the web server.

Question 657

Which of the following is the protocol data unit (PDU) of application layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 658

Which of the following technique is NOT used by a preacher against a Private Branch Exchange (PBX)?

- ☐ Eavesdropping
- ☐ Illegal call forwarding
- ☐ Forwarding a user's to an unused or disabled number
- ☐ SYN Flood

Question 659

Which of the following is the MOST likely reason why e-mail systems have become a useful source of evidence for litigation?

- ☐ Multiple cycles of backup files remain available.
- ☐ Access controls establish accountability for e-mail activity.
- ☐ Data classification regulates what information should be communicated via e-mail.
- ☐ Within the enterprise, a clear policy for using e-mail ensures that evidence is available.

Question 660

To minimize the cost of a software project, quality management techniques should be applied:

- ☐ as close to their writing (i.e., point of origination) as possible.
- ☐ primarily at project start-up to ensure that the project is established in accordance with organizational governance standards.
- ☐ continuously throughout the project with an emphasis on finding and fixing defects primarily during testing to maximize the defect detection rate.
- ☐ mainly at project close-down to capture lessons learned that can be applied to future projects.

Question 661

A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed NEXT to verify the adequacy of the new BCP?

- ☐ Full-scale test with relocation of all departments, including IT, to the contingency site
- ☐ Walk-through test of a series of predefined scenarios with all critical personnel involved
- ☐ IT disaster recovery test with business departments involved in testing the critical applications
- ☐ Functional test of a scenario with limited IT involvement

Question 662

Which of the following statement correctly describes the difference between IPSec and SSH protocols?

- ☐ IPSec works at the transport layer where as SSH works at the network layer of an OSI Model
- ☐ IPSec works at the network layer where as SSH works at the application layer of an OSI Model
- ☐ IPSec works at the network layer and SSH works at the transport layer of an OSI Model
- ☐ IPSec works at the transport layer and SSH works at the network layer of an OSI Model

Question 663

To ensure that audit resources deliver the best value to the organization, the FIRST step would be to:

- ☐ schedule the audits and monitor the time spent on each audit.
- ☐ train the IS audit staff on current technology used in the company.
- ☐ develop the audit plan on the basis of a detailed risk assessment.
- ☐ monitor progress of audits and initiate cost control measures.

Question 664

IT governance is PRIMARILY the responsibility of the:

- ☐ chief executive officer.
- ☐ board of directors.
- ☐ IT steering committee.
- ☐ audit committee.

Question 665

Which of the following methods of encryption has been proven to be almost unbreakable when correctly used?

- ☐ key pair
- ☐ Oakley
- ☐ certificate
- ☐ 3-DES
- ☐ one-time pad
- ☐ None of the choices.

Question 666

As an IS auditor it is very important to understand the importance of job scheduling. Which of the following statement is NOT true about job scheduler or job scheduling software?

- ☐ Job information is set up only once, which increase the probability of an error.
- ☐ Records are maintained of all job success and failures.
- ☐ Reliance on operator is reduced.
- ☐ Job dependencies are defined so that if a job fails, subsequent jobs relying on its output will not be processed.

Question 667

What are trojan horse programs?

- ☐ A common form of internal attack
- ☐ Malicious programs that require the aid of a carrier program such as email
- ☐ Malicious programs that can run independently and can propagate without the aid of a carrier program such as email
- ☐ A common form of Internet attack

Question 668

Which of the following is MOST critical for the successful implementation and maintenance of a security policy?

- ☐ Assimilation of the framework and intent of a written security policy by all appropriate parties
- ☐ Management support and approval for the implementation and maintenance of a security policy
- ☐ Enforcement of security rules by providing punitive actions for any violation of security rules
- ☐ Stringent implementation, monitoring and enforcing of rules by the security officer through access control software

Question 669

Which of the following is an implementation risk within the process of decision support systems?

- ☐ Management control
- ☐ Semistructured dimensions
- ☐ inability to specify purpose and usage patterns
- ☐ Changes in decision processes

Question 670

When auditing a proxy-based firewall, an IS auditor should:

- ☐ verify that the firewall is not dropping any forwarded packets.
- ☐ review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- ☐ verify that the filters applied to services such as HTTP are effective.
- ☐ test whether routing information is forwarded by the firewall.

Question 671

When should reviewing an audit client's business plan be performed relative to reviewing an organization's IT strategic plan?

- ☐ Reviewing an audit client's business plan should be performed before reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed after reviewing an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed during the review of an organization's IT strategic plan.
- ☐ Reviewing an audit client's business plan should be performed without regard to an organization's IT strategic plan.

Question 672

Which of the following is protocol data unit (PDU) of transport layer in TCP/IP model?

- ☐ Data
- ☐ Segment
- ☐ Packet
- ☐ Frame

Question 673

IS management is considering a Voice-over Internet Protocol (VoIP) network to reduce telecommunication costs and management asked the IS auditor to comment on appropriate security controls. Which of the following security measures is MOST appropriate?

- ☐ Review and, where necessary, upgrade firewall capabilities
- ☐ Install modems to allow remote maintenance support access
- ☐ Create a physically distinct network to handle VoIP traffic
- ☐ Redirect all VoIP traffic to allow clear text logging of authentication credentials

Question 674

Which of the following ACID property in DBMS requires that each transaction is "all or nothing"?

- ☐ Atomicity
- ☐ Consistency
- ☐ Isolation
- ☐ Durability

Question 675

Who assumes ownership of a systems-development project and the resulting system?

- ☐ User management
- ☐ Project steering committee
- ☐ IT management
- ☐ Systems developers

Question 676

During Involuntary termination of an employee, which of the following is the MOST important step to be considered?

- ☐ Get a written NDA agreement from an employee
- ☐ Terminate all physical and logical access
- ☐ Provide compensation in lieu of notice period
- ☐ Do not communicate to the respective employee about the termination

Question 677

An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?

- ☐ False-acceptance rate (FAR)
- ☐ Equal-error rate (EER)
- ☐ False-rejection rate (FRR)
- ☐ False-identification rate (FIR)

Question 678

Who should be responsible for network security operations?

- ☐ Business unit managers
- ☐ Security administrators
- ☐ Network administrators
- ☐ IS auditors

Question 679

Which of the following statement correctly describes the difference between black box testing and white box testing?

- ☐ Black box testing focuses on functional operative effectiveness where as white box assesses the effectiveness of software program logic
- ☐ White box testing focuses on functional operative effectiveness where as black box assesses the effectiveness of software program logic
- ☐ White box and black box testing focuses on functional operative effectiveness of an information systems without regard to any internal program structure
- ☐ White box and black box testing focuses on the effectiveness of the software program logic

Question 680

In which of the following WAN message transmission technique does two network nodes establish a dedicated communications channel through the network before the nodes may communicate?

- ☐ Message Switching
- ☐ Packet switching
- ☐ Circuit switching
- ☐ Virtual Circuits

Question 681

A hardware control that helps to detect errors when data are communicated from one computer to another is known as a:

- ☐ duplicate check.
- ☐ table lookup.
- ☐ validity check.
- ☐ parity check.

Question 682

Which of the following would be the MOST secure firewall system?

- ☐ Screened-host firewall
- ☐ Screened-subnet firewall
- ☐ Dual-homed firewall
- ☐ Stateful-inspection firewall

Question 683

The MOST important reason for an IS auditor to obtain sufficient and appropriate audit evidence is to:

- ☐ comply with regulatory requirements.
- ☐ provide a basis for drawing reasonable conclusions.
- ☐ ensure complete audit coverage.
- ☐ perform the audit according to the defined scope.

Question 684

What can be used to gather evidence of network attacks?

- ☐ Access control lists (ACL)
- ☐ Intrusion-detection systems (IDS)
- ☐ Syslog reporting
- ☐ Antivirus programs

Question 685

When identifying an earlier project completion time, which is to be obtained by paying a premium for early completion, the activities that should be selected are those:

- ☐ whose sum of activity time is the shortest.
- ☐ that have zero slack time.
- ☐ that give the longest possible completion time.
- ☐ whose sum of slack time is the shortest.

Question 686

What is the lowest level of the IT governance maturity model where an IT balanced scorecard exists?

- ☐ Repeatable but Intuitive
- ☐ Defined
- ☐ Managed and Measurable
- ☐ Optimized

Question 687

The MAJOR consideration for an IS auditor reviewing an organization's IT project portfolio is the:

- ☐ IT budget.
- ☐ existing IT environment.
- ☐ business plan.
- ☐ investment plan.

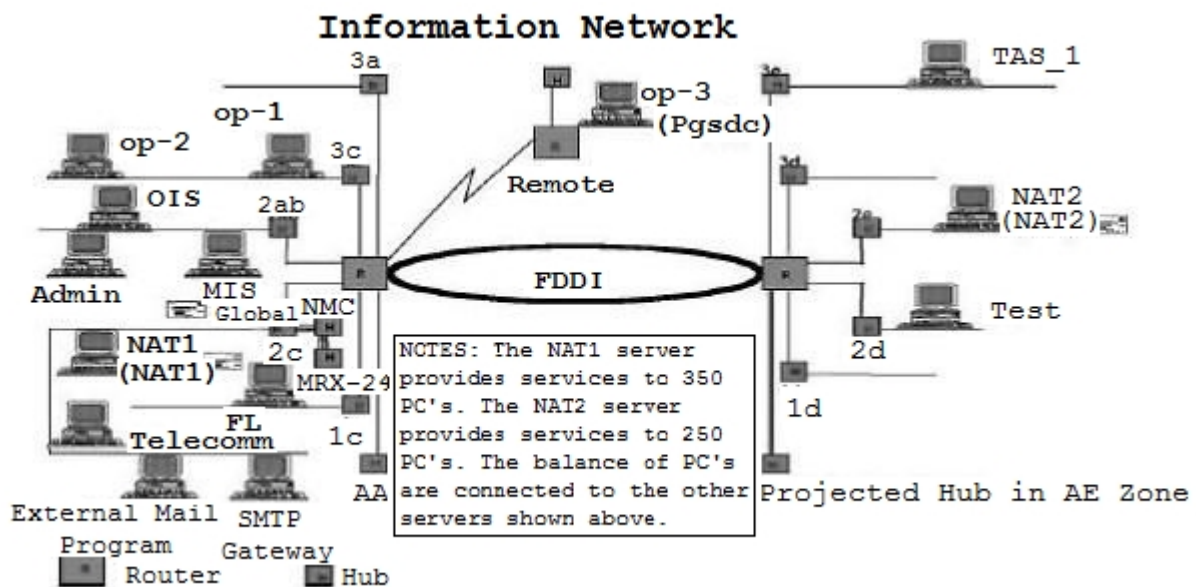
Question 688

To address an organization's disaster recovery requirements, backup intervals should not exceed the:

- ☐ service level objective (SLO).
- ☐ recovery time objective (RTO).
- ☐ recovery point objective (RPO).
- ☐ maximum acceptable outage (MAO).

Question 689

In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?



- ☐ Virus attack
- ☐ Performance degradation
- ☐ Poor management controls
- ☐ Vulnerability to external hackers

Question 690

Which of the following is the MOST reliable form of single factor personal identification?

- ☐ Smart card
- ☐ Password
- ☐ Photo identification
- ☐ iris scan

Question 691

Which of the following is the MOST effective control when granting temporary access to vendors?

- ☐ Vendor access corresponds to the service level agreement (SLA).
- ☐ User accounts are created with expiration dates and are based on services provided.
- ☐ Administrator access is provided for a limited period.
- ☐ User IDs are deleted when the work is completed.

Question 692

In a botnet, mailbot logs into a particular type of system for making coordinated attack attempts. What type of system is this?

- ☐ Chat system
- ☐ SMS system
- ☐ Email system
- ☐ Log system
- ☐ Kernel system
- ☐ None of the choices.

Question 693

Which of the following is often used as a detection and deterrent control against Internet attacks?

- ☐ Honeypots
- ☐ CCTV
- ☐ VPN
- ☐ VLAN

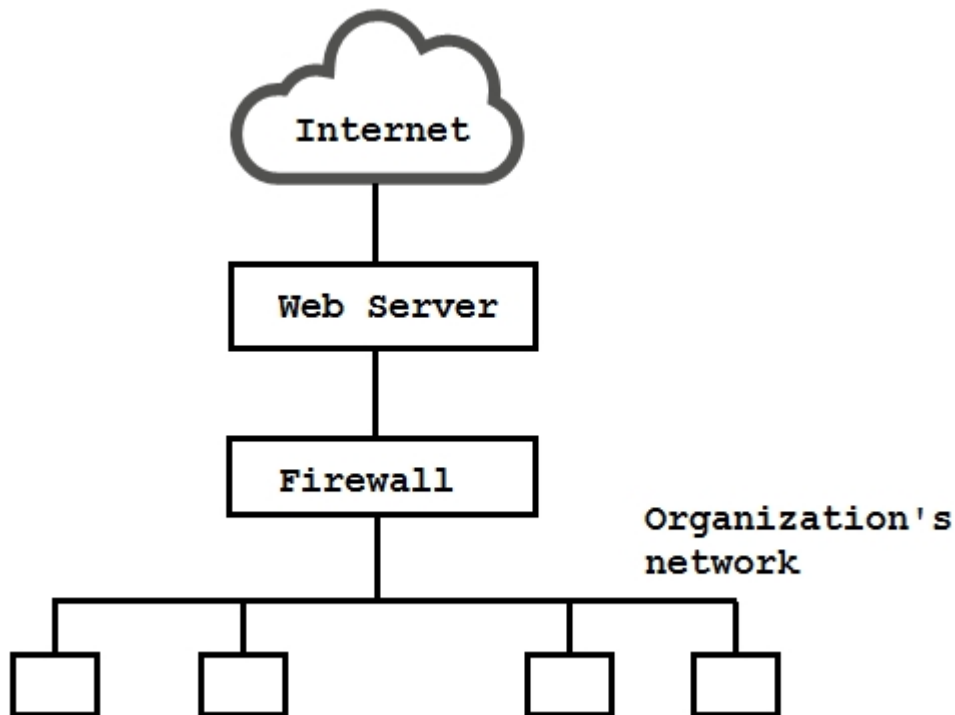
Question 694

Which of the following do digital signatures provide?

- ☐ Authentication and integrity of data
- ☐ Authentication and confidentiality of data
- ☐ Confidentiality and integrity of data
- ☐ Authentication and availability of data

Question 695

E-mail traffic from the Internet is routed via firewall-1 to the mail gateway. Mail is routed from the mail gateway, via firewall-2, to the mail recipients in the internal network. Other traffic is not allowed. For example, the firewalls do not allow direct traffic from the Internet to the internal network.



The intrusion detection system (IDS) detects traffic for the internal network that did not originate from the mail gateway. The FIRST action triggered by the IDS should be to:

- ☐ alert the appropriate staff.
- ☐ create an entry in the log.
- ☐ close firewall-2.
- ☐ close firewall-1.

Question 696

Which of the following is a guiding best practice for implementing logical access controls?

- ☐ Implementing the Biba Integrity Model
- ☐ Access is granted on a least-privilege basis, per the organization's data owners
- ☐ Implementing the Take-Grant access control model
- ☐ Classifying data according to the subject's requirements

Question 697

Which of the following layer from an enterprise data flow architecture captures all data of interest to an organization and organize it to assist in reporting and analysis?

- ☐ Desktop access layer
- ☐ Data preparation layer
- ☐ Core data warehouse
- ☐ Data access layer

Question 698

The BEST overall quantitative measure of the performance of biometric control devices is:

- ☐ false-rejection rate.
- ☐ false-acceptance rate.
- ☐ equal-error rate.
- ☐ estimated-error rate.

Question 699

Which of the following is penetration test where the penetration tester is provided with limited or no knowledge of the target's information systems?

- ☐ External Testing
- ☐ Internal Testing
- ☐ Blind Testing
- ☐ Targeted Testing