1 Q: The number one priority of disaster planning should always be:
A Preservation of capital
B Personnel evacuation and safety
C Resumption of core business functions
D Investor relations
2 Q: Which of the following is NOT a goal of a Business Impact Assessment (BIA)?
A To inventory mutual aid agreements
B To identify and prioritize business critical functions
C To determine how much downtime the business can tolerate
D To identify resources required by critical processes
3 Q: In the context of Data Processing Continuity Planning, “Subscription Services” refers to:
A Contracts to have replacement computer hardware within 72 hours
B Contracts to have replacement computer hardware within 24 hours
C Commercial services providing hot sites, warm sites, and cold sites
D The quarterly journal “Continuity Planning”
4 Q: The primary difference between a hot site and a warm site is:
A A hot site is closer to the organization’s data centers than is the warm site.
B The warm site’s systems don’t have the organization software or data installed.
C The warm site doesn’t have computer systems in it.
D The warm site is powered down, but the hot site is powered up and ready to go.
5 Q: Which of the following is NOT a concern for a hot site?
A Programs and data at the hot site must be protected.
B A widespread disaster will strain the hot site’s resources.
C A hot site is expensive because of the controls and patches required.
D Computer equipment must be shipped quickly to the hot site for it to be effective.
6 Q: The disaster recovery plan needs to be continuously maintained because:
A The organization’s software versions are constantly changing.
B The organization’s business processes are constantly changing.
C The available software patches are constantly changing.
D The organization’s data is constantly changing.
7 Q: How is the organization’s DRP best kept up-to-date?
A With regular audits to ensure that changes in business processes are known
B By maintaining lists of current software versions, patches, and configurations
C By maintaining personnel contact lists
D By regularly testing the DRP
8 Q: Multiple versions of a DRP available in the organization will:
A Allow older pass-along versions of the plan to circulated to some personnel
B Give involved personnel a choice of response procedures
C Cause confusion during a disaster
D Give critical personnel the best composite view of response procedures
9 Q: BCP stands for:
A Basic Continuity Planning
B Basic Continuity Procedure
C Business Continuity Procedure
D Business Continuity Planning
10 Q: “Remote journaling” refers to:
A A mechanism that transmits transactions to an alternate processing site
B A procedure for maintaining multiple copies of change control records
C A procedure for maintaining multiple copies of configuration management records
D A mechanism that ensures the survivability of written records
11 Q: Backing up data by sending it through a communications line to a remote location is known as:

A Transaction journaling
B Off-site storage
C Electronic vaulting
D Electronic journaling
12 Q: Which of the following is NOT a method used to create an online redundant data set?
A Remote journaling
B Off-site storage
C Electronic vaulting
D Database mirroring
13 Q: One of the chief disadvantages of a Mutual Aid Agreement is:
A There is no guarantee that the other organization will agree to help.
B A large disaster affecting both organizations renders the agreement worthless.
C It’s the most expensive way to acquire a warm site.
D The DRP isn’t tested until a disaster strikes.
14 Q: A hot site is the most expensive because:
A Travel costs can be high.
B Duplicate staff salaries are high.
C HVAC systems are expensive to operate.
D It requires constant maintenance to keep systems in sync.
15 Q: The types of DRP tests are:
A Checklist, walkthrough, simulation, parallel, and full interruption
B Checklist, simulation, parallel, and full interruption
C Checklist, walkthrough, simulation, and full interruption
D Walkthrough, simulation, and parallel
16 Q: A parallel DRP test:
A Is resource intensive and rarely used
B Tests the full responsiveness by shutting down production systems
C Runs in parallel with production processing
D Is a paper exercise to test theoretical response to a disaster
17 Q: A DRP checklist test:
A Is really only a review of the disaster recovery procedures
B Is a test of back-up system business resumption procedures
C Is a test of production system recovery procedures
D Is a test of business process failover procedures
18 Q: What is the purpose of a Salvage Team?
A To resume critical business operations at the alternate processing site
B To retrieve any needed items from off-site storage
C To return the primary processing site to normal business operations
D To salvage any usable or marketable assets after a disaster
19 Q: What is the purpose of a Recovery Team?
A To resume critical business operations at the alternate processing site
B To retrieve any needed items from off-site storage
C To return the primary processing site to normal business operations
D To salvage any usable or marketable assets after a disaster
20 Q: Why is communications with the media important during a disaster?
A Emergency communications with personnel occur through the media.
B The media can report official status instead of relying upon rumors.
C It’s required by the Securities and Exchange Commission.
D It’s recommended by the Business Contingency Planning Association.
21 Q: When is a disaster defined to be over?
A One year after it began
B When the Recovery phase has begun
C When all business operations have resumed at alternate operations site(s)
D When all business operations have resumed at the primary operations site(s)
22 Q: What new scenario did the 2001 World Trade Center disaster bring to business contingency
planning?

A The sudden loss of a significant portion of an organization’s workforce
B Airplanes being deliberately crashed into buildings
C The unprecedented cessation of securities trading for several consecutive days
D The restrictions of long-distance travel by air
23 Q: A data processing facility on truck trailers or mobile homes is known as:
A A Frozen Back-up Site
B A Migrant Back-up Site
C A Rolling Back-up Site
D In Itinerant Back-up Site
24 Q: What is the purpose of a Criticality Survey?
A It identifies the funding paths required during a disaster.
B It identifies the critical personnel in the organization.
C It identifies the critical path to full disaster recovery.
D It identifies the processes and functions that are critical to business operations.
25 Q: Which is NOT a factor in Business Contingency Planning?
A Making sure there are sufficient personnel to recover business operations.
B Identifying critical business processes and planning for their resumption
C Filing the Business Contingency Plan with local government authorities
D Identifying funding necessary during a disaster and for recovery of operations.
26 Q: What is the purpose of a Business Impact Assessment?
A To identify critical processes and the resources required to resume them
B To identify the impact of a disaster on the organization’s value chain
C To identify the financial cost of any particular disaster scenario
D To identify a disaster’s impact on company market share
27 Q: Typically the first step in the BCP process is:
A To inventory all business critical processes
B Scope and Plan Initiation
C Business Impact Analysis
D Business Continuity Plan
28 Q: Civil and criminal penalties can be imposed upon public companies that fail to maintain adequate
controls according to:
A HIPAA
B The Graham-Leach-Bliley Act of 1999
C The Information Controls and Practices Act of 1997
D The Foreign Corrupt Practices Act of 1977
29 Q: The loss of competitive advantage and market share is known as:
A A critical support area
B A qualitative loss
C A quantitative loss
D A nonproductive loss
30 Q: Acting with excellence, competence, and diligence is known as:
A Due care
B Due diligence
C Due ignorance
D The Golden Principles
31 Q: An access control system that grants access to information based upon its classification and the
clearance of the individual is known as:
A Identity-based access control
B Mandatory access control
C Role-based access control
D Identity-based access control
32 Q: An access control system that grants access to information based upon the identity of the user is
known as:

A Identity-based access control
B Mandatory access control
C Role-based access control
D Clearance-based access control
33 Q: An access control system that gives the user some control over who has access to information is
known as:
A Identity-based access control
B User-directed access control
C Role-based access control
D Clearance-based access control
34 Q: Encryption, tokens, access control lists, and smart cards are known as:
A Discretionary access controls
B Physical controls
C Technical controls
D Administrative controls
35 Q: Supervision, audits, procedures, and assessments are known as:
A Discretionary access controls
B Safeguards
C Physical controls
D Administrative controls
36 Q: Security guards, locked doors, and surveillance cameras are known as:
A Site-access controls
B Safeguards
C Physical access controls
D Administrative controls
37 Q: Role-based access control and task-based access control are examples of:
A Mandatory access controls
B Administrative controls
C Discretionary access controls
D Non-discretionary access controls
38 Q: Audits, background checks, video cameras, and listening devices are known as:
A Discretionary controls
B Physical controls
C Preventive controls
D Detective controls
39 Q: Smart cards, fences, guard dogs, and card key access are known as:
A Mandatory controls
B Physical controls
C Preventive controls
D Detective controls
40 Q: Is identification weaker than authentication?
A Yes: Identity is based only on the assertion of identity without providing proof.
B Yes: Identification uses ASCII data, whereas authentication uses binary data.
C No: Identification and authentication provide the same level of identity.
D No: They are used in different contexts and have nothing to do with each other.
41 Q: Two-factor authentication is so-called because:
A It requires two of the three authentication types.
B Tokens use two-factor encryption to hide their secret algorithms.
C Authentication difficulty is increased by a factor of two.
D It uses a factor of two prime numbers algorithm for added strength.
42 Q: “Something you are” refers to:
A A user’s security clearance
B A user’s role
C Type 2 authentication
D Type 3 authentication

43 Q: Two-factor authentication is stronger than single-factor authentication because:
A It uses a factor of two prime numbers algorithm for added strength.
B It relies upon two factors, such as a password and a smart card.
C Authentication difficulty is increased by a factor of two.
D The user must be physically present to authenticate.
44 Q: Finger print, retina scan, and facial scans are examples of:
A Biometric authentication
B Physical controls
C Type 2 authentication
D Three-factor authentication
45 Q: Tokens, smart cards, and ATM cards are examples of:
A Logical controls
B Identifiers
C Something you have
D Type 3 authentication
46 Q: Single sign-on performs which of the following:
A Stores the password locally using a “Save my password” feature.
B Permits authentication to applications without having to log in one by one.
C Stores the password and uses a cookie for subsequent authentication.
D Is no longer used because it is not secure.
47 Q: Which of the following is NOT a weakness in Kerberos?
A The user’s secret key is transmitted over the network.
B Kerberos is vulnerable to replay attacks.
C The TGS and AS servers are vulnerable to physical attack.
D The user’s secret key is temporarily stored on the client system.
48 Q: The definition of TACACS is:
A Technical Authentication Center Access Control Service
B Terminal Access Controller Authentication Control Service
C Technical Assistance Center Access Control System
D Terminal Access Controller Access Control System
49 Q: RADIUS is an example of:
A Remote Authentication and Dial-In User Service
B Centralized access control
C Distributed access control
D Detective control
50 Q: CHAP is used for:
A Centralized access control
B Encrypting RADIUS authentication
C Ciphering RADIUS authentication
D Creating one-time passwords
51 Q: RACF is used for:
A Providing Kerberos authentication
B Providing biometric authentication
C Providing access control in UNIX environments
D Providing access control services in IBM mainframe environments
52 Q: A system used to identify anomalies on a network is known as a:
A Signature-based intrusion detection system
B Network-based intrusion detection system
C Signature-based intrusion detection system
D Network-based intrusion control system
53 Q: One disadvantage of host-based intrusion detection is that:
A Event correlation is not possible.
B It cannot detect broadcast packets.
C It consumes resources on the host.
D It can only perform signature-based detection.
54 Q: One disadvantage of signature-based intrusion detection is that:
A It cannot recognize attacks that are not in the signature file.
B It detects intrusions only on hosts but not on networks.
C It detects intrusions only on networks but not on hosts.
D It can only detect mechanized attacks but not hacker attacks.
55 Q: The most common relational database manipulation and definition language in use is:

A DBML
B SQL Server
C SQL
D Oracle
56 Q: What is the value of a database view?
A It gives the DBA a top-down view of the schema.
B It defines which tables, records, and fields that a person may view.
C It is used to gather database security statistics.
D It gives the security administrator a graphic view of the permission tree.
57 Q: Object-oriented databases:
A Are well suited to the storage and manipulation of complex data types.
B Use fewer system resources than relational databases.
C Are easier to learn than relational databases.
D Have severe restrictions on the types and sizes of data elements.
58 Q: Which of the following is NOT a characteristic of biometrics?
A It can experience high false negatives.
B It can experience high false positives.
C Throughput rates are not an issue.
D Biometric databases can become very large.
59 Q: One of the difficulties associated with network-based intrusion detection systems is:
A Synchronizing the signature file with the firewall.
B The steep learning curve associated with IDS.
C The high number of false negatives that must be eliminated.
D The high number of false positives that must be eliminated.
60 Q: Which of the following is NOT an obstacle to implementing two-factor authentication?
A The need to integrate two-factor authentication into systems and applications.
B The high cost of implementation.
C Integrating two-factor authentication into the building’s badge entry system.
D The increased TCO over single-factor authentication.
61 Q: A database containing the data structures used by an application is known as:
A A data encyclopedia
B A data dictionary
C Metadata
D A schema
62 Q: The purpose of a Service Level Agreement is:
A To guarantee a minimum quality of service for an application or function
B To guarantee the maximum quality of service for an application or function
C To identify gaps in availability of an application
D To correct issues identified in a security audit
63 Q: CRCs, parity checks, and checksums are examples of:
A Corrective application controls
B Message digests
C Preventive application controls
D Detective application controls
64 Q: Data mining:
A Can be performed by privileged users only
B Is generally performed after hours because it’s resource intensive
C Refers to searches for correlations in a data warehouse
D Is the term used to describe a hacker who has broken into a databas
65 Q: “Object-oriented” and “relational” are examples of:
A Types of database tables
B Types of database records
C Types of database queries
D Types of databases
66 Q: Neural networking gets its name from:
A The make and model of equipment in a network

B Patterns thought to exist in the brain
C Its inventor, Sigor Neura
D Observed patterns in neural telepathy
67 Q: The verification activity associated with coding is called:
A Unit testing
B Design review
C System testing
D Architecture review
68 Q: What is the primary input of a high-level product design?
A Feasibility study
B Integration rules
C Unit testing
D Requirements
69 Q: The main improvement of the Waterfall software lifecycle model over earlier models was:
A System and software requirements are combined into one step.
B Developers can back up one step in the process for rework.
C Coding and testing is combined into one step.
D The need for rework was eliminated.
70 Q: The primary feature of the Spiral software development model is that:
A It shows cumulative project cost over several development iterations.
B It includes Risk Analysis as a milestone.
C It includes Security Assessment as a milestone.
D It is only suitable for software integration, not software development.
71 Q: Which of the following is NOT a value of change control in the software development lifecycle?
A Changes are documented and subject to approval.
B Scope creep is controlled.
C It gives the customer veto power over proposed changes.
D The cost of changes is considered.
72 Q: How does the Waterfall software development lifecycle help to assure that applications will be
secure?
A Security requirements can be included early on and verified later in testing.
B The testing phase includes penetration testing.
C The Risk Analysis phase will uncover flaws in the feasibility model.
D A list of valid users must be approved prior to production.
73 Q: The main purpose of configuration management is to:
A Require cost justification for any change in a software product
B Require approval for any desired change in a software product
C Maintain a detailed record of changes for the lifetime of a software product.
D Provide the customer with a process for requesting configuration changes.
74 Q: Configuration management can include an approval-based check-in/check-out mechanism to
ensure that:
A Developers won’t make unapproved changes to software.
B All changes have been tested.
C All changes have been approved.
D All changes have been verified.
75 Q: The Software Capability Maturity Model is a measure of:
A Advancements in software capabilities
B The technical capabilities of software
C The maturity of an organization’s software development processes
D The ability of a software product to remain accurate even after many years
76 Q: The components of the SEI Process Improvement IDEAL Model are:
A Initiate, Diagnose, Establish, Action, and Leverage
B Identify, Document, Establish, Annotate, and Learn
C Influence, Diagnose, Establish, Annotate, and Learn

D Identify, Document, Elucidate, Annotate, and Launch
77 Q: Which of the following is NOT a goal of the Software Capability Maturity Model?
A Reduced development time
B Improved development tools
C Improved software quality
D Improved planning
78 Q: The top-most level in the Software Capability Maturity Model has to do with:
A Continuous and institutionalized process improvement
B Complete lack of processes and controls
C Fully normalized and optimized software
D Fully tested and validated software
79 Q: The purpose of a Build List is:
A To obtain approval at the Detailed Design step of the software lifecycle
B To ensure that the compiler includes all necessary components during a build
C To ensure that all the necessary components are present during a build
D A record of the versions of all components of each copy of a product
80 Q: In which steps are Security Specifications used in the software lifecycle?
A Coding only
B Product Design only
C Product Design and Detailed Design
D Product Design, Detailed Design, and Coding
81 Q: What is the purpose of a Software Library?
A It’s an official software source code repository.
B It’s a location where developers can store tools, code fragments, and utilities.
C It’s the location where unit test plans are developed.
D It’s the local copy of the Software Vault.
82 Q: Objects in object-oriented systems communicate with other objects via:
A Named pipes
B Queues
C Pipes
D Messages
83 Q: The software code in an object-oriented environment is known as the:
A Code
B Method
C Instance
D Behavior
84 Q: The maturity levels in the Software CMM are
A Reactive, Proactive, Managed, and Optimizing
B Reactive, Responsive, Defined, Managed, and Optimizing
C Initiating, Defined, Repeatable, Managed, and Optimizing
D Initiating, Repeatable, Defined, Managed, and Optimizing
85 Q: Software products are the most secure when:
A They’re run in B2 environments.
B They’re run in C2 environments.
C Security requirements and architectures are known as early as possible.
D Security is layered in as the last step of development.
86 Q: The platform-independent mechanism developed by the OMG is:
A CORBA
B COBRA
C VIPER
D DCOM
87 Q: Fuzzification is most often used in:
A Synaptic networks
B Magnetic media degaussers
C Expert systems

D Database caching algorithms
88 Q: The term “sandbox” is used to describe:
A The portion of virtual memory that maps to physical memory
B The closed environment in which a Java applet runs
C The location where temporary compilation files are stored
D The location where developers write and test code
89 Q: Which of the following is NOT a security concern about ActiveX?
A ActiveX has a robust sandbox that protects the rest of the system.
B There is no way to prevent malicious ActiveX code from damaging a client.
C An ActiveX control has complete access to the entire client system.
D The digital signature on an ActiveX control only tells it is genuine.
90 Q: RAID is also known as:
A Recoverable Array of Independent Disks
B Risk Analysis Initiation Detail
C Redundant Array of Independent Disks
D Robust Array of Inexpensive Disks
91 Q: The process of breaking the key and/or plaintext from an enciphered message is known as:
A Decryption
B Steganography
C Cryptanalysis
D Extraction
92 Q: The method of encryption in which both sender and recipient possess a common encryption key
is known as:
A Message digest
B Hash function
C Public key cryptography
D Secret key cryptography
93 Q: Why would a user’s public encryption key be widely distributed?
A So that cryptographers can attempt to break it.
B Because it’s encrypted.
C Because the user’s private key can’t be derived from their private key.
D So that the user can decrypt messages from any location.
94 Q: Reading down the columns of a message that has been written across is known as:
A A columnar transposition cipher
B Calculating the hash
C Calculating the checksum
D Calculating the modulo
95 Q: An asymmetric cryptosystem is also known as:
A Message digest
B Hash function
C Public key cryptosystem
D Secret key cryptosystem
96 Q: The process of hiding a message inside of a larger dataset is known as:
A Decryption
B Steganography
C Cryptanalysis
D Extraction
97 Q: Steganography is not easily noticed because:
A Monitor and picture quality are so good these days.
B Most PCs’ speakers are turned off or disabled.
C The human eye often can’t sense the noise that steganography introduces.
D Checksums can’t detect most steganographed images.
98 Q: What historic event was the backdrop for breakthroughs in strategic cryptography?
A The Gulf War
B World War I
C World War II

D The Six Day War
99 Q: Non-repudiation refers to:
A The technology that shoots down the “I didn’t send that message” excuse
B Re-verification of all CA certificate servers
C The annual competency review of system and network authentication mechanisms
D The annual competency review of system and network authentication mechanisms
100 Q: The amount of effort required to break a given ciphertext is known as the:
A Work function
B Effort function
C Cryptanalysis
D Extraction
101 Q: What is one disadvantage of an organization signing its own certificates?
A The certificate signing function is labor intensive.
B Anyone outside the organization will receive warning messages.
C The user identification process is labor intensive.
D It is much more expensive than having certificates signed by a CA.
102 Q: The ability for a government agency to wiretap a data connection is implemented in the:
A Skipjack chip
B Magic lantern
C Cutty chip
D Clipper chip
103 Q: The cipher device used by Germany in World War II is known as:
A M-922
B M-902
C Enigma
D Turing
104 Q: The problem of WTLS-to-SSL transactions existing temporarily “in the clear” is called the:
A GATT GAP
B Knapsack problem
C WEP GAP
D WAP GAP
105 Q: Why would a user’s public encryption key be widely distributed?
A So that cryptographers can attempt to break it.
B Because it’s encrypted.
C So that any person can send an encrypted message to the user.
D So that the user can decrypt messages from any location.
106 Q: Which of the following is NOT a solution for securing e-mail?
A MIME Object Security Services (MOSS)
B S/MIME
C SET
D PGP
107 Q: An algorithm that is easy to compute in the “forward” direction but difficult to compute
“backwards” is known as:
A A block grant
B A stream cipher
C A public key function
D A one-way function
108 Q: What technology advancement led to the breaking of DES?
A VLSI chips
B Decrease in cost of computers
C Neural networks
D Expert systems
109 Q: Why does PGP not scale well in larger environments?
A Users certify each other, which can result in too large a web of trust.
B The system or security administrator must manually sign every new key.

C Storing the public keys will take more space than previously believed.
D Not enough computing power exists to encrypt and decrypt all the e-mail traffic.
110 Q: What party in an organization signs a subscriber’s digital certificate?
A Repository
B Subscriber’s supervisor
C Subscriber
D Certificate Authority
111 Q: The science of hiding the true meaning of messages from unintended recipients is known as:
A Cryptosystem
B Cryptology
C Cryptography.
D Enciphering
112 Q: Which protocol is most often used to access certificates in a PKI?
A SSL
B LDAP
C CA
D SSH
113 Q: One of the challenges facing participants in a symmetric key cryptosystem is:
A How to tell each user which algorithm to use
B How to safely transmit the secret key to each user
C How to transmit enciphered messages
D How to store deciphered messages
114 Q: The type of encryption used by Caesar is:
A One=Time Pad
B Transposition
C Transformation
D Substitution
115 Q: Which of the following is NOT a purpose of a digital signature?
A Authentication to a key server
B Detecting unauthorized changes of data
C Non-repudiation
D Identifying the person who signed the data
116 Q: A given symmetric cryptosystem uses a 64 bit key size. If an asymmetric cryptosystem is used
instead, what key size is required that will give the equivalent strength of the symmetric
cryptosystem?
A 2048 bits
B 512 bits
C 64 bits
D 24 bits
117 Q: How can symmetric key cryptosystems be made more secure?
A By periodically changing the secret key
B By periodically changing the length of the secret key
C By canceling and reissuing secret keys
D By periodically changing the encryption algorithm
118 Q: A cipher that rearranges the order of characters from the original message is a:
A Substitution
B Transfiguration
C Transubstantiation
D Transposition
119 Q: Which public key cryptosystems relies upon the difficulty of factoring the product of large prime
numbers?
A El Gamal
B Elliptic Curve
C RSA
D Diffie-Hellman

120 Q: The substitution cipher used by UNIX systems that shifts characters by 13 positions is known as:
A Crypt
B ROOT 13
C ROT 13
D ROTOR 13
121 Q: The Internet Worm Incident of 1988 was perpetrated by:
A The 414 Gang
B Robert Morris
C Kevin Mitnick
D Gene Spafford
122 Q: Forensics is the term that describes:
A Due process
B Tracking hackers from other countries
C Taking steps taken to preserve and record evidence
D Scrubbing a system in order to return it to service
123 Q: An expert witness:
A Offers an opinion based upon the facts of a case and upon personal expertise
B Is someone who was present at the scene of the crime
C Has direct personal knowledge about the event in question
D Can testify in criminal proceedings only
124 Q: A witness:
A Offers an opinion based upon the facts of a case and upon personal expertise
B Is someone who was present at the scene of the crime
C Has direct personal knowledge about the event in question
D Can testify in criminal proceedings only
125 Q: “Entrapment” is defined as:
A Leading someone to commit a crime that they wouldn’t otherwise have committed.
B Monitoring with the intent of recording a crime
C Paying someone to commit a crime
D Being caught with criminal evidence in one’s possession
126 Q: “Enticement” is defined as:
A Being caught with criminal evidence in one’s possession
B Leading someone to commit a crime that they wouldn’t otherwise have committed.
C Monitoring with the intent of recording a crime
D Keeping the criminal at the scene of the crime long enough to gather evidence.
127 Q: The purpose of a honeypot is to:
A Log an intruder’s actions.
B Act as a decoy to keep the intruder interested while his origin and identity are traced.
C Deflect denial of service attacks away from production servers.
D Provide direct evidence of a break-in.
128 Q: Which of the following is NOT a precaution that needs to be taken before monitoring e-mail?
A Strict procedures that define under what circumstances e-mail may be searched.
B A visible notice stating that e-mail is company information subject to search.
C Issue monitoring tools to all e-mail administrators.
D Make sure that all employees know that it’s being monitored.
129 Q: Intellectual property laws apply to:
A Trade secrets, trademarks, copyrights, and patents.
B Trademarks, copyrights, and patents.
C Trademarks only.
D Patents only.
130 Q: In order to be admissible, electronic evidence must:
A Be legally permissible
B Not be copied
C Have been in the custody of the investigator at all times

D Not contain viruses
131 Q: Who has jurisdiction over computer crimes in the United States?
A The Department of Justice
B The Electronic Crimes Task Force
C Any state or local jurisdiction
D The FBI and the Secret Service
132 Q: Under what circumstance may evidence be seized without a warrant?
A If it’s in the public domain
B If it’s believed that its destruction is imminent
C In international incidents
D If it’s on a computer
133 Q: Motive, means, and opportunity:
A Are required prior to the commission of a crime
B Are the required three pieces of evidence in any criminal trial
C Are the three factors that determine whether someone may have committed a crime.
D Are the usual ingredients in a sting operation
134 Q: Using social skills to acquire critical information about computer systems is known as:
A Social espionage
B Social engineering
C Social racketeering
D Eavesdropping
135 Q: It is difficult to determine that theft of information has occurred because:
A It’s not a crime unless someone posts the information on the Internet.
B Most sites have inadequate audit logs.
C More often than not, the information is still there.
D Most law enforcement personnel don’t understand information technology.
136 Q: The illegal acquisition of funds through manipulation or falsification of financial information is
known as:
A Embezzlement
B Conspiracy
C Blackmail
D Extortion
137 Q: The illegal acquisition of funds through intimidation is known as:
A Embezzlement
B Conspiracy
C Blackmail
D Extortion
138 Q: The categories of common law that relate to information systems are:
A Patent, copyright, and trademark
B Misdemeanor and felony
C Criminal and civil
D Criminal, civil, regulatory, intellectual property, and privacy
139 Q: The primary goal of information privacy laws is:
A To require organizations to ask for permission each time they share information
B To discourage the abuse of individuals’ private information
C To require the use of government-operated databases instead of private databases
D To prevent individuals from falsifying information about themselves
140 Q: The chain of evidence ensures:
A That evidence links the alleged perpetrator to the crime
B That those who collected it will be available to testify in court
C That it’s relevant and reliable
D The integrity of evidence, from collection through safekeeping
141 Q: The only way to be absolutely sure that a hard disk has not been tampered with is to:
A Write-protect the hard disk

B Remove the hard disk from the computer
C Create a digital signature based upon its entire contents
D Back it up to tape and make comparisons later as needed
142 Q: A set of values defining acceptable and unacceptable behavior is known as:
A Ethics
B Guiding principles
C Laws
D Requirements
143 Q: During an interrogation of a suspect, copies of any evidence should be used because:
A The suspect may ask for the evidence.
B The suspect may attempt to destroy the evidence.
C The original should be locked in the evidence room.
D The suspect be allowed to give a copy of the evidence to his attorney.
144 Q: Federal Sentencing Guidelines specify that a corporation's senior officers can be:
A Imprisoned for failing to protect corporate information assets from harm
B Held personally liable for failing to protect information assets from harm.
C Sentenced to house arrest for failing to protect information assets from harm.
D Barred from management for failing to protect information assets from harm.
145 Q: The owner of a patent is protected for how long in the United States?
A 17 years
B 7 years
C 10 years
D 27 years
146 Q: Laws having to do with a wrong that one has inflicted upon another are called:
A Statutory laws
B Common laws
C Civil laws
D Liability laws
147 Q: The US government program requiring shielding and other mechanisms designed to prevent the
emanation of radio frequency (RF) signals generated by computer equipment is called:
A AURORA
B TEAPOT
C RIVEST
D TEMPEST
148 Q: The deliberate misuse of information is prohibited by:
A The US Federal Trade Commission
B The Heisenberg Principle
C The Fourth Amendment of the United States Constitution
D The (ISC)2 Code of Ethics
149 Q: The name of the law requiring protection of personal medical information is:
A UCITA
B HAPPY
C HIPAA
D HIIPA
150 Q: The primary drawback to the FBI's Carnivore capability is:
A It's useless if those observed encrypt their data.
B It takes too long to crack most encryption schemes.
C It noticeably degrades performance.
D It doesn't work on Windows systems.
151 Q: Access controls and card key systems are examples of:
A Detective controls
B Preventative controls

C Corrective controls
D Trust controls
152 Q: Audit trails and security cameras are examples of:
A Detective controls
B Preventative controls
C Corrective controls
D Trust controls
153 Q: Reboot instructions and file restore procedures are examples of:
A Detective controls
B Preventative controls
C Corrective controls
D Trust controls
154 Q: Covert channel analysis is used to:
A Detect and understand unauthorized communication
B Encipher unauthorized communications
C Decipher unauthorized communications
D Recover unauthorized communications
155 Q: Least privilege means:
A Analysis that determines which privileges are required to complete a task.
B Persons with higher privileges delegate some of those privileges to others.
C The persons with the fewest access rights do all the work.
D Users should have the minimum privileges required to perform required tasks.
156 Q: The practice of “separation of duties”:
A Is used to provide variety by rotating personnel among various tasks.
B Helps to prevent any individual from compromising an information system.
C Is used to ensure that the most experienced persons get the best tasks.
D Is used in large 24x7 operations shops.
157 Q: Which of the following tasks would NOT be performed by a security administrator?
A Changing file permissions
B Configuring user privileges
C Installing system software
D Reviewing audit data
158 Q: What is the potential security benefit of “rotation of duties”?
A It reduces the risk that personnel will perform unauthorized activities.
B It ensures that all personnel are familiar with all security tasks.
C It is used to detect covert activities.
D It ensures security because personnel are not too familiar with their duties.
159 Q: The process of reviewing and approving changes in production systems is known as:
A Availability management
B Configuration management
C Change management
D Resource control
160 Q: The process of maintaining versions of software versions and settings is known as:
A Availability management
B Configuration management
C Change management
D Resource control
161 Q: Configuration management is used to:
A Document the approval process for configuration changes
B Control the approval process for configuration changes
C Ensure that changes made to an information system don’t compromise its security.
D Preserve a complete history of the changes to software or data in a system.

162 Q: The traces of original data remaining after media erasure is known as:
A Data remanence
B Data traces
C Leakage
D Data particles
163 Q: Software controls are used to:
A Perform input checking to ensure that no buffer overflows occur
B Keep running programs from viewing or changing other programs’ memory.
C Perform configuration management-like functions on software
D Ensure the confidentiality and integrity of software
164 Q: Someone who is performing penetration testing is:
A Stress-testing access controls
B Looking for vulnerabilities in computer hardware or software
C Looking for unauthorized modems and wireless network base stations
D Attempting to decrypt encrypted data
165 Q: Which of the following is NOT a purpose for audit trails?
A Determining why a transaction was performed
B Event reconstruction
C Tracing transaction history
D Determining what or who performed a transaction
166 Q: The primary reason for using an external auditor versus an internal auditor is:
A Prestige
B Expertise
C Objectivity
D Expense
167 Q: Password cracking, port scanning, and network sniffing are known as:
A Covert channels
B Threats
C Vulnerabilities
D Weaknesses
168 Q: Software bugs, configuration errors, and the absence of security processes are known as:
A Covert channels
B Threats
C Vulnerabilities
D Inverse channels
169 Q: A port scanning tool is used to:
A Configure network ports on a system
B Discover files and directories with wide-open permissions
C Capture network traffic for subsequent analysis
D Discover weaknesses in systems
170 Q: A sniffer is used to:
A Configure network ports on a system
B Discover files and directories with wide-open permissions
C Capture network traffic for subsequent analysis
D Discover weaknesses in systems
171 Q: A sniffer program is used by an intruder to:
A Diagnose network problems
B Remotely sniff a network that he doesn’t have physical access to
C Discover files and directories with wide-open permissions
D Discover weaknesses in systems
172 Q: Which of the following is NOT a security issue regarding single-user mode?
A Authentication is disabled on all network services such as Telnet and FTP.
B The administrator has full root privileges and can make system changes.
C Security features are disabled in single-user mode.
D The administrator can transmit information off the system without a trace.
173 Q: Fraud is a term used to describe:

A Stealing of information to sell to a competitor or other person
B Activities such as denial of service, social engineering, or eavesdropping
C Siphoning money out of an organization via phony transactions
D Any activity that takes advantage of weaknesses and results in personal gain
174 Q: Denial of service is:
A The result when an administrator disables unnecessary network services
B An attack that prevents legitimate users from being able to use a resource
C What happens when a user lacks sufficient security credentials
D What happens when you left your shoes off when ordering pizza over the Web.
175 Q: The purpose of intrusion detection is:
A To detect attacks and other anomalies
B To make sure that people aren't trying to "tailgate" through security entrances
C To verify that the honeypot or honeynet is working correctly
D To catch the hacking attempts that the firewall missed
176 Q: The main disadvantage of signature-based intrusion detection is:
A It's considerably more expensive than linguistic intrusion detection.
B Some hackers are good at forging other people's signatures.
C Signatures must be constantly kept up-to-date.
D Handwriting tablets are still too expensive.
177 Q: "War driving" is the term used to describe:
A Looking for vulnerable client systems in order to build a list of DDOS zombies.
B Sniffing wireless networks to look for vulnerabilities
C Running multiple concurrent port scanning tools on a system
D Running DOOM™ on a Gigabit Ethernet
178 Q: Violation processing is used to:
A Quantify security risks
B Attempt to bypass intrusion detection systems
C Discover hard-to-guess passwords
D Detect individuals who are generating a high volume of errors.
179 Q: Which of the following is NOT an environmental concern for long-term media storage?
A Temperature
B Humidity
C Lumens
D EMF
180 Q: Maintenance accounts shouldn't be used by applications because:
A Applications would be operating in full privileged mode, bypassing all security.
B Too many people have the password to the maintenance account.
C Maintenance accounts utilize write-behind transactions, resulting in data loss.
D Maintenance accounts run at too low a priority.
181 Q: Why should a data center's walls go all the way to the ceiling and not just stop as high as the
suspended ceiling?
A The walls will be stronger.
B The HVAC will run more efficiently.
C An intruder could otherwise enter the data center by climbing over the wall.
D The high wall will block more noise.
182 Q: Why should a data center's walls go all the way to the ceiling and not just stop as high as the
suspended ceiling?
A The walls will serve as an effective fire break.
B The HVAC will run more efficiently.
C The walls will be stronger.
D The high wall will block more noise.
183 Q: Drain pipes that channel liquids away from a building are called:

A Positive drains
B Tight lines
C Storm drains
D Negative drains
184 Q: Of what value is pre-employment screening?
A Undesirable medical or genetic conditions could diminish productivity.
B Only certain personality types work in some organizations.
C Employees need to have knowledge of security.
D Background checks and reference checks could uncover undesirable qualities.
185 Q: Which of the following is NOT a part of a building's automated access audit log?
A Time of the attempted entry
B The reason for the attempted entry
C Location of attempted entry
D Entry success or failure
186 Q: "Tailgating" is a term describing what activity?
A Logging in to a server from two or more locations.
B Causing a PBX to permit unauthorized long distance calls.
C Following an employee through an uncontrolled access
D Following an employee through a controlled access
187 Q: What does "fail open" mean in the context of controlled building entrances?
A Controlled entrances permit no one to pass.
B Controlled entrances permit people to pass without identification.
C A power outage won't affect control of the entrance.
D A pass key is required to enter the building.
188 Q: What does "fail closed" mean in the context of controlled building entrances?
A Controlled entrances permit no one to pass.
B Controlled entrances permit people to pass without identification.
C The access control computer is down.
D Everyone is permitted to enter the building.
189 Q: A water sprinkler system characterized as always having water in the pipes is known as:
A Dry pipe
B Wet pipe
C Preaction
D Discharge
190 Q: A water sprinkler system that charges the pipes upon receiving a heat or smoke alarm and then
discharges at a higher temperature is known as:
A Dry pipe
B Wet pipe
C Preaction
D Discharge
191 Q: Why would a dry pipe sprinkler be preferred over a wet pipe sprinkler?
A Dry pipe systems put out a fire more quickly.
B Dry pipe systems consume less water.
C There is a smaller likelihood of rust damage.
D There is a potentially useful time delay before water is discharged.
192 Q: How does water aid in fire suppression?
A It reduces the fire's oxygen supply.
B It isolates the fire's fuel supply.
C It lowers the temperature needed to sustain the fire.
D It extinguishes the fire through a chemical reaction.
193 Q: Which of the following are NOT fire detectors?
A Dial-up alarms
B Heat-sensing alarms
C Flame-sensing alarms
D Smoke-sensing alarms
194 Q: Which of the following is NOT a physical site security measure?
A Guards

B Fencing
C Warning signs
D CCTV
195 Q: What physical control element is most useful in an emergency?
A Security camera
B Security guards
C Guard dogs
D Barricades
196 Q: How does CO2 aid in fire suppression?
A It reduces the fire’s oxygen supply.
B It isolates the fire’s fuel supply.
C It lowers the temperature needed to sustain the fire.
D It extinguishes the fire through a chemical reaction.
197 Q: Why should computer and office equipment be checked in and checked out at a building
entrance?
A So that IT will know if it’s available in the event of a disaster.
B Fixed asset personnel can keep location records up-to-date.
C Accountability: To discourage employees from trying to sneak equipment out.
D To account for what would otherwise be metal detector alarms.
198 Q: What is the principal feature of a mantrap?
A Its advanced metal detecting capability.
B Only one of its two doors can be opened at once.
C The high speed by which people can enter and exit a facility.
D Its biometric identifying capabilities.
199 Q: To what height should critical building be illuminated at night?
A 4 feet
B 8 feet
C 12 feet
D 24 feet
200 Q: What is considered sufficient fencing to keep out determined intruders?
A 12 feet
B 6 feet
C 12 feet with 1 strand of barbed wire
D 8 feet high with 3 strands of barbed wire
201 Q: What is considered the most effective form of magnetic media erasure?
A Physical destruction
B Degaussing
C Overwriting
D Relabeling
202 Q: Standards for magnetic media reuse specify what minimum for magnetic media reuse?
A Degauss the media 3 times
B Degauss the media 7 times
C Overwrite or format the media 7 times
D Overwrite or format the media 21 times
203 Q: How does soda acid aid in fire suppression?
A It reduces the fire’s oxygen supply.
B It isolates the fire’s fuel supply.
C It lowers the temperature needed to sustain the fire.
D It extinguishes the fire through a chemical reaction.
204 Q: What is the purpose of off-site media storage?
A An alternate back-up media set in the event of a program bug
B An alternate back-up media set in the event of an operator error
C An alternate back-up media set in the event of a catastrophic hardware failure
D An alternate back-up media set in the event that the data center is destroyed
205 Q: What is one possible weakness of a BIOS password intending to protect hard disk data?

A It may be possible to read the hard disk data by placing it in another computer.
B It might not be providing disk encryption, but only a login feature.
C The encryption used is generally weak.
D It can be defeated by connecting jumpers together on the system board.
206 Q: What is the greatest source of loss when a corporate laptop is lost or stolen?
A The gold that can be recovered by melting the system down
B The RAM chips
C The value of the information stored on it
D The black market value of the LCD screen
207 Q: What are the various types of motion detectors?
A Wave patterns and radar
B Audio, wave patterns, and capacitance
C Infrared and capacitance
D Audio and capacitance
208 Q: Which of the following is NOT a characteristic of passive electronic access cards?
A They contain batteries that must be changed or charged.
B They are powered by the RF field transmitted by the reader.
C They transmit at a frequency different from the frequency emitted by the reader.
D They need not touch the reader but work by proximity.
209 Q: Which of the following is NOT a characteristic of active electronic access cards?
A They contain batteries that must be changed or charged.
B They’re powered by the RF field transmitted by the reader.
C They transmit at a frequency different from the frequency emitted by the reader.
D They need not touch the reader, but work by proximity.
210 Q: Which of the following is NOT an advantage of cipher locks over access card locks?
A Cipher locks are independent and work even when centralized systems can’t.
B A cipher lock may be more cost-effective than an access card lock for one door.
C Cipher locks offer better centralized control than do access card locks.
D Cipher locks are self-contained, requiring no external power or wired.
211 Q: Memory that is used to store computer instructions and data is known as:
A UART
B SIMM
C Cache
D ROM
212 Q: Firmware is generally stored on:
A ROM or EPROM
B Tape
C RAM
D Any removable media
213 Q: What is the purpose of memory protection?
A It protects memory from malicious code.
B It prevents a program from being able to access memory used by another program.
C Memory protection is another term used to describe virtual memory backing store.
D It assures that hardware refresh is frequent enough to maintain memory integrity.
214 Q: The mapping of existing physical memory into a larger, imaginary memory space is known as:
A Virtual memory
B Swapping
C Thrashing
D Spooling

215 Q: Vendor-independent systems with published specifications are known as:
A Open source
B RFCs
C Freeware
D Open systems
216 Q: Which of the following is NOT a security issue with distributed architectures?
A Lack of security awareness by some personnel
B Difficulty in controlling the distribution and use of software
C Protection of centrally stored information
D Backups might not be performed on some systems, risking loss of data
217 Q: TCB is an acronym for:
A Trusted Computing Baseline
B Trusted Computing Base
C Tertiary Computing Base
D Trusted Cache Base
218 Q: The sum total of all protection mechanisms in a system is known as a:
A Trusted Computing Base
B Protection domain
C Trusted path
D SPM (Summation Protection Mechanism)
219 Q: The mechanism that overlaps hardware instructions to increase performance is known as:
A RISC
B Pipeline
C Pipe dream
D Multitasking
220 Q: FORTRAN, BASIC, and C are known as:
A Dead languages
B Living languages
C Second-generation languages
D Third-generation languages
221 Q: The purpose of an operating system is to:
A Manage hardware resources
B Compile program code
C Decompile program code
D Present graphic display to users
222 Q: Protection rings are used for:
A Implementing memory protection
B Creating nested protection domains
C Modeling layers of protection around an information object
D Shielding systems from EMF
223 Q: The TCSEC document is known as the Orange Book because:
A It’s orange in color.
B It covers the major classes of computing system security, D through A.
C Its coverage of security was likened to the defoliant Agent Orange.
D No adequate model of computing system security was available at the time.
The Orange Book was one of several books in the Rainbow Series, each describing various levels
and contexts of computer security, and each with its own unique color.
224 Q: A chart of capabilities and subjects is known as a(n):
A Protection ring
B Chart of accounts
C Access control list
D Access matrix
225 Q: The model that assigns classification levels to materials and to individuals to determine who can
view materials based upon their classification is known as:
A The DoD multilevel security model
B The Bell-LaPadula Model
C The Clark-Wilson Model

D The Information Flow Model
226 Q: The model that incorporates constrained data items and procedures for verifying and changing
integrity states is known as:
A The Bell-LaPadula Integrity Model
B The Clark-Wilson Integrity Model
C The Wilson-Phillips Integrity Model
D The Information Flow Model
227 Q: The Bell-LaPadula model is an example of:
A An accreditation model
B A Take-Grant model
C An integrity model
D An access control model
228 Q: Information flow models are used to:
A Understand where information is flowing in a system
B Ensure that information can flow only in directions permitted by security policy
C Ensure that information can flow only from higher to lower integrity levels
D Verify that information is properly classified
229 Q: The Biba Integrity Model is:
A An extension of the Bell-LaPadula Access Control Model
B A modern version of the Clark-Wilson Integrity Model
C The private industry version of the Clark-Wilson Integrity Model
D The de facto standard for modeling information flow
230 Q: A evaluation of security features in an information system against a set of security requirements
is known as a(n):
A Protection
B Certification
C Accreditation
D Verification
231 Q: A declaration that an information system is approved for a particular function is known as a(n):
A Protection
B Certification
C Accreditation
D Verification
232 Q: Dedicated, compartmented, controlled, and multilevel mode are examples of:
A Security labels
B Security levels
C Security modes
D Rings
233 Q: The security mode where all users have the required clearance to access information is known as:
A Dedicated
B Compartmented
C Trusted
D Labeled
234 Q: The security mode where all users have the required clearance and authorization to access
information is known as:
A Dedicated
B Compartmented
C Trusted
D Labeled
235 Q: “Fail closed” is defined as:
A The state entered by the takover node in a fault-tolerant cluster.
B The state entered by a failed node in a fault-tolerant cluster.
C The failure of a component that results in information being available.
D The failure of a component that results in information being unavailable.

236 Q: “Fail open” is defined as:
A The state entered by the takover node in a fault-tolerant cluster
B The state entered by a failed node in a fault-tolerant cluster
C The failure of a component that results in information being available
D The failure of a component that results in information being unavailable
237 Q: An unintended and unauthorized communication path is known as a:
A Covert channel
B Back door
C Front door
D Side door
238 Q: A component or feature of an information system that permits someone or something to bypass
security controls is known as a:
A Trap door
B Back door
C Front door
D Side door
239 Q: A system consisting of proprietary components is known as:
A An open system
B A closed system
C A commercial system
D A for-profit system
240 Q: The communications channel that connects the various components of a computer system is
known as a:
A Star
B Ring
C Bus
D Plane
241 Q: Of what value is separation of authority in an organization?
A It limits the capabilities of any single individual.
B It provides multiple paths for fulfilling critical tasks.
C It accommodates the requirement for parallel audit trails.
D It ensures that only one person is authorized to perform each task.
242 Q: The term “open view” refers to what activity?
A Reclassifying a document so that anyone may view it.
B Viewing the contents of one’s private encryption key.
C Leaving classified information where unauthorized persons can see them.
D Using a decryption key to view the contents of a message.
243 Q: Which individual is responsible for classifying information?
A Owner
B Custodian
C Creator
D User
244 Q: Which individual is responsible for protecting information?
A Owner
B Custodian
C Creator
D User
245 Q: Which of the following is NOT a criterion for classifying information?
A Marking
B Useful life
C Value
D Age
246 Q: What is the purpose of a senior management statement of security policy?
A It defines who is responsible for carrying out a security policy.
B It states that senior management need not follow a security policy.
C It emphasizes the importance of security throughout an organization.
D It states that senior management must also follow a security policy.
247 Q: What is the purpose of an “advisory policy”?

A This is an optional policy that can be followed.
B This is an informal offering of advice regarding security practices.
C This is a temporary policy good only for a certain period of time.
D This is a policy that must be followed but is not mandated by regulation.
248 Q: What is the definition of a “threat”?
A Any event that produces an undesirable outcome.
B A weakness present in a control or countermeasure.
C An act of aggression that causes harm.
D An individual likely to violate security policy.
249 Q: A weakness in a security control is called a:
A Risk
B Vulnerability
C Threat
D Hole
250 Q: A security control intended to reduce risk is called a:
A Safeguard
B Threat
C Countermeasure
D Partition
251 Q: The purpose of risk analysis is:
A To qualify the classification of a potential threat.
B To quantify the likelihood of a potential threat.
C To quantify the net present value of an asset.
D To quantify the impact of a potential threat.
252 Q: Annualized Rate of Occurrence refers to:
A The exact frequency of a threat.
B The estimated frequency of a threat.
C The estimated monetary value of a threat.
D The exact monetary value of a threat.
253 Q: Single Loss Expectancy refers to:
A The expectation of the occurrence of a single loss.
B The monetary loss realized from an individual threat.
C The likelihood that a single loss will occur.
D The annualized monetary loss from a single threat.
254 Q: Annualized Loss Expectancy refers to:
A The expectation of the occurrence of losses throughout the year.
B The monetary loss expected from all occurrences of a single threat.
C The total monetary annual loss from all occurrences of a single threat.
D An industry-provided benchmark that serves as a prediction of a threat.
255 Q: Which of the following is NOT required when performing a Risk Analysis?
A Determine the monetary value of an asset.
B Identify all threats to an asset.
C Classify the asset’s security level.
D Calculate the Annualized Loss Expectancy.
256 Q: Which of the following is NOT a general remedy to risk?
A Risk mitigation
B Risk transference
C Risk acceptance
D Risk reduction
257 Q: What is meant by the term “risk reduction”?
A Factoring risk downward to match return on investment (ROI).
B Removal of threats from the Risk Analysis (RA).
C Reducing risk by lowering the Annualized Loss Expectancy (ALE).
D Measures that are taken to reduce the risk of loss to an asset.
258 Q: What factors are used to select a safeguard?
A Cost-benefit analysis, accuracy, and auditability.
B Net present value, accuracy, and auditability.
C Annualized Loss Expectancy, Exposure Factor, and the value of the asset.
D The monetary cost of the safeguard.

259 Q: What is the best reason for employees to be aware of an organization’s security policies?
A So they can socialize it with other employees.
B To receive reminders of best security practices.
C So they can perform the right actions needed to protect information.
D So they can avoid the consequences of not knowing the security policies.
260 Q: What is the purpose of a “back door”?
A It is an alternate means of authentication.
B It is used to permit a function when the security officer is absent.
C It is used to bypass the guarded main entrance of a secure facility.
D It is used to bypass one or more security controls.
261 Q: What is meant by the term “risk mitigation”?
A Elimination of risk.
B Reduction of risk to an acceptable level.
C Calculating vulnerabilities multiplied by threats.
D Ranking risks in order of likelihood.
262 Q: What is the purpose of a security guideline?
A It provides suggested methods for following a security policy.
B It explains the purpose of a security policy.
C It explains why a security policy must be followed.
D It describes the consequences for violating a security policy.
263 Q: A statement that specifies specific security technologies or products is known as a:
A Product guideline
B Informative policy
C Security standard
D Safeguard
264 Q: Information containing salaries of employees would most likely be classified as:
A Sensitive
B Private
C Confidential
D Top Secret
265 Q: The purpose of a security control is to:
A Contain and deliver a specific security policy.
B Record recipients of classified documents.
C Properly release data to comply with a court order.
D Reduce threats and vulnerabilities to an acceptable level.
266 Q: The most cost-effective way to make employees aware of security policies is to:
A Use e-mail and Web sites to communicate the importance of security.
B Enroll all employees in a security awareness class.
C Send a hardcopy set of security policies to each employee.
D Purchase a good book on security for each employee.
267 Q: Information warfare is BEST known as a:
A Potential loss
B Vulnerability
C Threat
D Risk
268 Q: Which of the following is NOT a part of risk analysis?
A To determine value of assets
B To determine the location of assets
C To determine threats to assets
D To select safeguards
269 Q: What is a PSE?
A Preferred Security Examination
B Preliminary Security Examination
C Potential Security Event
D Probably Security Event
270 Q: The term “unclassified” refers to:
A Documents that have yet to be classified.
B Secret information that has not received its permanent classification.
C Policies that refer to public concerns on privacy.

D Documents that are designated as not sensitive.
271 Q: UDP is sometimes called the “unreliable data protocol” because:
A It works only on low-speed wireless LANs.
B UDP packets rarely get through because they have a lower priority.
C Few know how to program UDP.
D UDP does not guarantee delivery.
272 Q: TCP is a poor choice for streaming video because:
A It is too bursty for large networks.
B Acknowledgement and sequencing add significantly to its overhead.
C Checksums in video packets are meaningless.
D TCP address space is nearly exhausted.
273 Q: The purpose of Layer 1 in the OSI model is to:
A Transmit and receive bits.
B Sequence packets and calculate checksums.
C Perform application-to-application communications.
D Transmit and receive frames.
274 Q: How many layers does the TCP/IP protocol model have?
A 4
B 5
C 6
D 7
275 Q: ARP is:
A Access Routing Protocol
B Address Resolution Protocol
C Access Resolution Protocol
D Address Recovery Protocol
276 Q: What is the purpose of ARP?
A When given an IP address, ARP returns a MAC address.
B When given a MAC address, ARP returns an IP address.
C It calculates the shortest path between two nodes on a network.
D It acquires the next IP address on a circular route.
277 Q: What is the purpose of RARP?
A When given an IP address, ARP returns a MAC address.
B When given a MAC address, ARP returns an IP address.
C It traces the source address of a spoofed packet.
D It determines the least cost route through a multipath network.
278 Q: 132.116.72.5 is a:
A MAC address
B IPv4 address
C Subnet mask
D Ipv6 address
279 Q: 04:c6:d1:45:87:E8 is a:
A MAC address
B IPv4 address
C Subnet mask
D Ipv6 address
280 Q: The “ping” command sends:
A IGRP Echo Reply packets
B IGRP Echo Request packets
C ICMP Echo Request packets
D UDP Echo Request packets
281 Q: SMTP is used to:
A Manage multiple telnet sessions.
B Tunnel private sessions through the Internet.
C Simulate modems.
D Transport e-mail.
282 Q: Which of the following is a disadvantage of SSL?
A It requires a certificate on every client system.
B It is CPU intensive.
C All clients must be retrofitted with HTTP v3 browsers.
D An eavesdropper can record and later play back an SSL session.
283 Q: An access control list is NOT used by:
A A firewall or screening router to determine which packets should pass through.

B A router to determine which administrative nodes may access it.
C A bastion host to determine which network services should be permitted.
D A client system to record and save passwords.
284 Q: Stateful inspection firewalls:
A Are no longer used because all network traffic is stateless.
B Record the state of each packet in their logs.
C Are slower than simple packet filtering firewalls.
D Are easier to manage because their rulesets are self-healing.
285 Q: The purpose of a bastion host is to:
A Be a backup firewall should the main firewall fail or become overloaded.
B Host internet-facing services.
C Serve as the security management server.
D Serve as the firewall management server.
286 Q: What is the purpose of NAT?
A It is used to convert a session’s private IP address to a public address.
B It is used to detect spoofed IP packets.
C It is used to counterattack hacking attempts.
D It is used to facilitate court-ordered wiretaps.
287 Q: 10.20.30.40 is an example of:
A A Boolean operator on a complex firewall rule.
B A subnet mask.
C The default step function for VPN encryption.
D A private, non-routable IP address.
288 Q: Which of the following is NOT a VPN protocol standard?
A L2TP
B IPSec
C P3P
D PPTP
289 Q: Which of the following cable types is most easily tapped by eavesdroppers?
A RG11
B UTP
C Coax
D STP
290 Q: Ethernet is an example of:
A A mesh topology network
B A BUS topology network
C A ring topology network
D A tree topology network
291 Q: The biggest disadvantage of callback security is:
A The caller can only call from a predetermined location.
B It only works in networks that support caller-ID.
C It is vulnerable to replay attack.
D It only works in networks that support *69 functionality.
292 Q: X.25 is an example of:
A A remote device management technology.
B A circuit-switched technology.
C A packet-switched technology.
D A digital certificate technology.
293 Q: Which of the following is NOT a private circuit technology?
A xDSL
B T3
C E1
D FR
294 Q: PAP is considered a weak authentication protocol because:
A It uses a static password that is not encrypted.
B It uses a changing, but predictable, password that is not encrypted.
C Its session keys are easily guessed.
D Only the first four characters of the password are significant.
295 Q: Most companies disallow POTS lines in offices because:
A Employees should not be running ISPs using company resources.

B EMF emanating from a POTS line can corrupt any nearby LANs.
C It would facilitate the installation of a rogue modem.
D It would facilitate the installation of an 802.11x APN.
296 Q: Extending the corporate network to a remote location is a description of:
A Remote access
B Routing
C Layer 3 switching
D Bridging
297 Q: Which of the following is NOT a remote access type?
A VDSL
B RADIUS
C Cable modem
D ISDN
298 Q: IPSsec, PPP, L2TP, and SLIP are examples of:
A Encapsulation protocols
B Authentication protocols
C Encryption algorithms
D Routing protocols
299 Q: The primary security benefit of a switched LAN versus a shared-media LAN is:
A Switches do not transmit spoofed IP packets.
B Broadcast packets are sent only to nodes on the local switch.
C Unlike a shared-media LAN, a network sniffer cannot capture all LAN traffic.
D Switches are not vulnerable to broadcast storms.
300 Q: Which of the following is NOT true of an Ethernet network?
A Ethernet is a broadcast medium.
B Ethernet is a switched medium.
C IP addresses can be forged on an Ethernet network.
D MAC addresses can be forged on an Ethernet network.
1 RIGHT=B
See Chapter 10. People always come first!
2 RIGHT=A
See Chapter 10. Mutual aid agreements are not a significant concern of a BIA.
3 RIGHT=C
See Chapter 10. Subscription services refers to hot sites, warm sites, and cold sites.
4 RIGHT=B
See Chapter 10. Warm sites are mostly like hot sites except that the organization’s software and data
aren’t on the warm site’s systems.
5 RIGHT=D
See Chapter 10. The hot site already has computer equipment.
6 RIGHT=B
See Chapter 10. The DRP must contain an up-to-date record of all critical business processes.
7 RIGHT=A
See Chapter 10. Audits will uncover changes that are needed in the DRP.
8 RIGHT=C
See Chapter 10. There should be only one available version of the DRP available in order to avoid
confusion.
9 RIGHT=D
BCP is an acronym for Business Continuity Planning. See Chapter 10.
10 RIGHT=A
See Chapter 10. Remote journaling keeps data at an alternate site up-to-date at all times.
11 RIGHT=C
See Chapter 10. Electronic vaulting is the term that describes backing up data over a
communications line to another location.
12 RIGHT=B

See Chapter 10. Off-site storage is merely an alternate location for storing back-up media.

13 RIGHT=B

See Chapter 10. A disaster large enough to affect both organizations will negate the plan.

14 RIGHT=D

See Chapter 10. The hot site systems’ hardware, software, applications, and patches must be kept current with the organization’s main data center(s).

15 RIGHT=A

See Chapter 10. The five types of DRP tests are checklist, walkthrough, simulation, parallel, and full interruption.

16 RIGHT=C

See Chapter 10. A parallel test utilizes parallel processing of the organization’s systems but without shutting down production systems.

17 RIGHT=A

See Chapter 10. A checklist test is nothing more than a review of disaster recovery procedures.

18 RIGHT=C

See Chapter 10. The purpose of the Salvage Team is to resume normal business operations at the primary processing site(s).

19 RIGHT=A

See Chapter 10. The Recovery Team’s purpose is to get critical business operations up and running as soon as possible at the alternate processing site.

20 RIGHT=B

See Chapter 10. In the absence of communication with the media, inaccurate and usually pessimistic news about the disaster will spread.

21 RIGHT=D

See Chapter 10. The disaster is said to be over when all business operations have resumed at their usual production sites.

22 RIGHT=A

See Chapter 10. Prior to 2001, business contingency planning didn’t adequately take into account the unlikely (but now proven possible) scenario of the loss of many or most of an organization’s personnel.

23 RIGHT=C

See Chapter 10. A Rolling Back-up Site (also known as a Mobile Back-up Site) is a portable site built onto a truck trailer or mobile home structure.

24 RIGHT=D

See Chapter 10. The Criticality Survey is used to identify all critical business processes and functions.

25 RIGHT=C

See Chapter 10. With rare exceptions, local governments aren’t involved in companies’ business contingency planning.

26 RIGHT=A

See Chapter 10. The main purpose of a Business Impact Assessment is the identification of critical business processes, the amount of downtime for those processes the business can tolerate, and the resources required to resume those critical processes.

27 RIGHT=B

See Chapter 10. The scope of the BCP program must first be determined.

28 RIGHT=D

See Chapter 10. The Foreign Corrupt Practices Act of 1977 imposes civil and criminal penalties on
publicly owned companies that fail to adequately control their information systems.
29 RIGHT=B
Qualitative losses, such as loss of competitive advantage, are more difficult to measure. See Chapter
10.
30 RIGHT=A
See Chapter 10. Executives and other managers must operate their companies with due care, which
includes having adequate disaster recovery planning.
31 RIGHT=B
See Chapter 3. Mandatory access control is based upon the user's clearance level, the classification
of the information, and the user's need to know.
32 RIGHT=A
See Chapter 3. Identity-based access control is used to grant access to information based upon the
identity of the person requesting access.
33 RIGHT=B
See Chapter 3. User-directed access control, a form of discretionary access control, permits the user
to grant access to information, based upon certain limitations.
34 RIGHT=C
See Chapter 3. These are examples of technical, or logical, controls.
35 RIGHT=D
See Chapter 3. Administrative access controls consist of all the policies and procedures that are used
to mitigate risk.
36 RIGHT=C
See Chapter 3. Physical access controls include these and others such as backups, protection of
cabling, and card key access.
37 RIGHT=D
See Chapter 3. These are known as non-discretionary controls, which match information to roles or
tasks and not individual users.
38 RIGHT=D
See Chapter 3. Detective controls are those controls that are designed to detect security events.
39 RIGHT=C
See Chapter 3. Preventive controls are those that are used to prevent security events.
40 RIGHT=A
See Chapter 3. Identification is only the assertion of identity, whereas authentication is the proof of
identity.
41 RIGHT=A
See Chapter 3. Two-factor authentication requires any two of Type 1 (Something you know), Type 2
(Something you have), and Type 3 (Something you are).
42 RIGHT=D
See Chapter 3. “Something you are” refers to authentication that measures something physical such
as a fingerprint, retina scan, or voiceprint.
43 RIGHT=B
See Chapter 3. Two-factor authentication requires any two of Type 1 (Something you know), Type 2
(Something you have), and Type 3 (Something you are).
44 RIGHT=A
See Chapter 3. These are all biometrics. Other examples include hand geometry scans, voice scans,
and signature scans.

45 RIGHT=C
See Chapter 3. These are examples of “Something you have,” also known as Type 2 authentication.
46 RIGHT=B
See Chapter 3. Single sign-on permits a user’s authentication to be granted to all participating
applications. This alleviates the problem of having to remember several different user-IDs and
passwords.
47 RIGHT=A
See Chapter 3. The user’s secret key is never transmitted over the network.
48 RIGHT=D
TACACS is an authentication protocol that stands for Terminal Access Controller Access Control
System .See Chapter 3.
49 RIGHT=B
See Chapter 3. RADIUS is used for centralized access control.
50 RIGHT=A
See Chapter 3. CHAP is used for centralized access control.
51 RIGHT=D
See Chapter 3. RACF, or Resource Access Control Facility, is a mainstay in IBM mainframe
environments for providing access control.
52 RIGHT=B
See Chapter 3. A network-based intrusion detection system (IDS) is used to detect possible
intrusions by using either signature-based or anomaly-based methods.
53 RIGHT=C
See Chapter 3. Host-based intrusion detection systems (IDS) consume resources on the host because
it must analyze potentially voluminous network traffic.
54 RIGHT=A
See Chapter 3. Signature-based intrusion detection systems (IDS) can only detect attacks that are
defined in its signature file. It can be a major pain to update signature files on all IDSs in the
organization.
55 RIGHT=C
See Chapter 3. SQL is used to build, manage, and update relational databases.
56 RIGHT=B
See Chapter 3. A database view is a virtual window into a database that permits the DBA to define
what tables, records, and fields a person can see.
57 RIGHT=A
See Chapter 3. Object-oriented databases are well suited for complex and large data types but take
far more system resources and have steep learning curves.
58 RIGHT=C
See Chapter 3. Throughput rates ARE an issue with biometrics.
59 RIGHT=D
See Chapter 3. IDS is known for a high number of false positives that must be eliminated one by
one.
60 RIGHT=C
See Chapter 3. Two-factor authentication is rarely (if ever) integrated with a badge entry system.
61 RIGHT=B
See Chapter 6. A data dictionary contains information about an application’s data structures,
including table names, field names, indexes, and so on.
62 RIGHT=A

See Chapter 6. A Service Level Agreement, or SLA, defines minimum performance metrics of an
application or service.
63 RIGHT=D
See Chapter 6. They are examples of detective application controls because they are designed to help
discover security breaches in a network.
64 RIGHT=C
See Chapter 6. Data mining is the term used to describe searches for correlations in a data
warehouse.
65 RIGHT=D
See Chapter 6. “Object-oriented” and “relational” are types of databases.
66 RIGHT=B
See Chapter 6. Neural networks are systems that can detect patterns after a period of training.
67 RIGHT=A
See Chapter 6. Unit testing is the testing of small modules of code, which is used to verify that the
coding was done correctly.
68 RIGHT=D
See Chapter 6. Requirements are the single largest input used in the high-level product design phase.
69 RIGHT=B
See Chapter 6. Going back one step for rework was the main improvement of the Waterfall model.
This is important because sometimes any of the steps may fail to consider something that the next
step uncovers.
70 RIGHT=A
See Chapter 6. Spiral software model depicts the accumulation of cost over the entire lifetime of a
software product.
71 RIGHT=C
See Chapter 6. Veto power is unlikely, but the other choices listed are value-added features of
change control.
72 RIGHT=A
See Chapter 6. The greatest value in the development lifecycle is getting security requirements in at
the beginning so that security will be “baked in.”
73 RIGHT=C
See Chapter 6. Configuration management produces a highly detailed record, including details of
each and every copy of a software product that was created.
74 RIGHT=A
See Chapter 6. A check-in/check-out mechanism in configuration management keeps the developers
from making unauthorized and undocumented “improvements.”
75 RIGHT=C
See Chapter 6. The Software Capability Maturity Model (SCMM) is a measure of an organization’s
software development process.
76 RIGHT=A
SEI’s IDEAL stands for Initiate, Diagnose, Establish, Action, and Leverage. See Chapter 6.
77 RIGHT=B
See Chapter 6. The SCMM has little, if anything, to do with development tools, but the other
answers are some of its objectives.
78 RIGHT=A
See Chapter 6. The highest order of existence in the SCMM is a model of continuous process

improvement.
79 RIGHT=D
See Chapter 6. The Build List is a part of Configuration Management that records all the component
versions for each build of the product.
80 RIGHT=B
See Chapter 6. Security Specifications are used during Product and Detailed Design.
81 RIGHT=A
See Chapter 6. The Software Library is a Configuration Management term describing the controlled
source code repository. Access to the Software Library is restricted.
82 RIGHT=D
See Chapter 6. “Message” is the term that describes object-to-object communication, which, by the
way, is technology independent.
83 RIGHT=B
See Chapter 6. A method is the code associated with an object.
84 RIGHT=D
See Chapter 6. The five maturity levels are (from lowest to highest) Initiating, Repeatable, Defined,
Managed, and Optimizing.
85 RIGHT=C
See Chapter 6. The most secure software is that which is built knowing all the security requirements
up front.
86 RIGHT=A
See Chapter 6. CORBA, or Common Object Request Broker Architecture, is the platformindependent
mechanism developed by the Object Management Group (OMG).
87 RIGHT=C
See Chapter 6. Fuzzification is used to determine the degree of truth in rule premises.
88 RIGHT=B
See Chapter 6. The sandbox is the space where a Java applet runs, thereby protecting the rest of the
system.
89 RIGHT=A
See Chapter 6. ActiveX has no sandbox; the other concerns are legitimate.
90 RIGHT=C
See Chapter 6. RAID is an acronym for Redundant Array of Independent Disks.
91 RIGHT=C
See Chapter 7. Cryptanalysis is the process of getting the key and/or the original message the hard
way.
92 RIGHT=D
See Chapter 7. Secret key cryptography is used when all parties possess a common key.
93 RIGHT=C
See Chapter 7. In public-key cryptography, the value of the public key doesn’t in any way betray the
value of the secret key.
94 RIGHT=A
See Chapter 7. In this cipher, the cryptographer writes across but reads down.
95 RIGHT=C
See Chapter 7. Asymmetric cryptosystems are also known as public key cryptosystems.
96 RIGHT=B
See Chapter 7. Steganography is the science of inserting messages into larger datasets so that the
existence of the message is unknown.

97 RIGHT=C

Steganography is difficult to detect visually in an image. See Chapter 7.

98 RIGHT=C

See Chapter 7. World War II saw a significant advancement in the science of cryptography. World War II became a war of cryptanalysis wherein each participant was sometimes able to break the code of the others, resulting in strategic advantage.

99 RIGHT=A

See Chapter 7. Non-repudiation helps to prove that a specific individual did create or sign a document or transmit data to or from another.

100 RIGHT=A

See Chapter 7. Work function is the term used to describe the amount of time and/or money required to break a ciphertext.

101 RIGHT=B

See Chapter 7. The lack of a top-level signature on a certificate results in warning messages stating that the certificate lacks a top-level signature.

102 RIGHT=D

See Chapter 7. The clipper chip is that which performs encryption but also provides a legal wiretap capability.

103 RIGHT=C

See Chapter 7. The famous German device is the Enigma.

104 RIGHT=D

See Chapter 7. The WAP GAP refers to the place in the overall architecture where an encrypted message exists unencrypted.

105 RIGHT=C

See Chapter 7. Wide distribution of a user’s public key permits anyone with the public key algorithm to encrypt a message intended for the user by using that person’s public key. Any such message can be decrypted only by someone possessing the user’s private key, which would presumably be only the user.

106 RIGHT=C

See Chapter 7. SET is a financial transaction security tool and is not used for e-mail.

107 RIGHT=D

See Chapter 7. A one-way function is easy to compute in the forward direction but very difficult to run backwards.

108 RIGHT=A

See Chapter 7. VLSI enables complex mathematical functions to be carried out in hardware at high speeds.

109 RIGHT=A

See Chapter 7. The web of trust can become very large and potentially weak in places.

110 RIGHT=D

See Chapter 7. The certificate authority, after receiving satisfactory proof of the identity of the individual, signs that individual’s certificate.

111 RIGHT=C

See Chapter 7. Cryptography is the art of hiding the meaning of messages so that unintended recipients can’t read them.

112 RIGHT=B

See Chapter 7. LDAP is the directory agent of choice for PKIs.

113 RIGHT=B

See Chapter 7. Getting the secret key to each user can be difficult because it must not be made
available to any unauthorized party.
114 RIGHT=D
See Chapter 7. Caesar used Substitution, specifically by shifting the alphabet by three letters.
115 RIGHT=A
See Chapter 7. This is a totally bogus answer, but the other three ARE stated uses of digital
signatures.
116 RIGHT=B
An asymmetric cryptosystem must use a 512 bit key size to match the strength of a symmetric
cryptosystem using a 64 bit key. See Chapter 7.
117 RIGHT=A
See Chapter 7. By changing the secret key periodically, only a finite portion of the ciphertext can be
broken by someone who has discovered the secret key.
118 RIGHT=D
See Chapter 7. Transposition is the process of changing the order of characters in a message.
119 RIGHT=C
See Chapter 7. RSA is the only one of these that works with the product of two prime numbers. The
others mentioned here use discreet logarithms in finite fields.
120 RIGHT=C
See Chapter 7. UNIX used the simple substitution cipher called ROT 13 to obfuscate messages. It
was most often used in newsgroups to hide off-color jokes from those who were easily offended and
didn’t wish to read them. ROT-13 was not meant to be difficult to decrypt -- only to make text
unrecognizable on sight.
121 RIGHT=B
See Chapter 11. Robert Morris wrote and released what is now known as the Internet Worm in 1988.
Gene Spafford wrote several papers on the topic.
122 RIGHT=C
See Chapter 11. Forensics is the study and activity of discovering, preserving, and recording
evidence.
123 RIGHT=A
See Chapter 11. An expert witness offers his opinion based upon the facts of the case and upon
personal expertise.
124 RIGHT=C
See Chapter 11. A witness testifies the facts as he understands them.
125 RIGHT=A
See Chapter 11. Entrapment refers to the activities that lure an individual into committing a crime
that they wouldn’t have otherwise committed.
126 RIGHT=D
See Chapter 11. Enticement is used to keep a criminal at the scene of the crime. In the context of
electronic crime, a honeypot is a great way to keep an intruder sniffing around while his origin is
traced.
127 RIGHT=B
See Chapter 11. A honeypot is designed to keep an intruder sniffing around long enough for
investigators to determine his origin and identity.
128 RIGHT=C
See Chapter 11. This is not a precaution at all – not even a step that would be considered. The other

items DO need to be taken before any monitoring is performed.
129 RIGHT=A
See Chapter 11. Intellectual property laws apply to trade secrets, trademarks, copyrights, and patents.
130 RIGHT=A
See Chapter 11. Evidence gathered in violation of any laws can't be admitted in court.
131 RIGHT=D
See Chapter 11. Believe it or not, the FBI and the Secret Service have jurisdiction over computer
crimes.
132 RIGHT=B
See Chapter 11. Evidence may only be seized if law enforcement believes that it's about to be
destroyed.
133 RIGHT=C
See Chapter 11. Motive, means, and opportunity are the standard criteria when considering a
possible suspect in a crime.
134 RIGHT=B
See Chapter 11. Social engineering is the term used to describe the activity carried out by clever
individuals who often claim to be someone that they are not in order to elicit information from
unsuspecting individuals who are just trying to be helpful.
135 RIGHT=C
See Chapter 11. When information is stolen, it's most often copied, which means that the original
information is still there, unaltered.
136 RIGHT=A
See Chapter 11. Embezzlement is basically stealing money from an organization by falsifying
records.
137 RIGHT=D
See Chapter 11. Unlike embezzlement (when the organization doesn't know that it's giving money
away), extortion means that the organization is paying someone to do (or not do) something.
138 RIGHT=D
See Chapter 11. Criminal, civil, and regulatory relate universally. Intellectual property and privacy
are especially applicable to information systems.
139 RIGHT=B
See Chapter 11. Privacy laws seek to curb the abuses of private information by organizations
wishing to misuse it.
140 RIGHT=D
See Chapter 11. The chain of evidence ensures its integrity from the place of collection through
preservation and finally presentation in court.
141 RIGHT=C
See Chapter 11. Although a tape backup could be used, a digital signature is by far the most reliable
way of determining whether a hard disk has been tampered with.
142 RIGHT=A
See Chapter 11. Ethics defines right and wrong behavior. Various organizations have codes of ethics
defining right and wrong in various contexts.
143 RIGHT=B
See Chapter 11. It would be a shame if a suspect destroyed evidence that investigators worked so
hard to produce.
144 RIGHT=B

See Chapter 11. Senior officers can be personally liable for up to $290 million for failure to comply
with the law.
145 RIGHT=A
See Chapter 11. Patents protect its owner for 17 years.
146 RIGHT=C
See Chapter 11. Laws having to do with one person or organization damaging another are civil laws.
147 RIGHT=D
See Chapter 11. TEMPEST is the name of the program that developed standards for shielding
facilities to prevent RF containing secret information from radiating from buildings.
148 RIGHT=D
The (ISC)2 Code of Ethics prohibits the deliberate misuse of information. See Chapter 11.
149 RIGHT=C
See Chapter 11. HIPAA, the Health Insurance Portability and Accountability Act, addresses health
care privacy.
150 RIGHT=A
See Chapter 11. Carnivore is the FBI’s means for wiretapping data transmissions. It’s pretty much
useless if the data being wiretapped is encrypted.
151 RIGHT=B
See Chapter 9. Preventative controls are those that are designed to prevent a security incident.
152 RIGHT=A
See Chapter 9. Detective controls are designed to record security events.
153 RIGHT=C
See Chapter 9. Corrective controls are used to resume business operations after a security incident.
154 RIGHT=A
See Chapter 9. Covert channel analysis is used to detect, understand, and help security personnel to
prevent covert channels.
155 RIGHT=D
See Chapter 9. Least privilege is the principle that states that users should have access only to the
data and functions required for their duties.
156 RIGHT=B
See Chapter 9. Separation of duties is used to ensure that no single individual has too much
privilege, which could lead to a security incident.
157 RIGHT=C
See Chapter 9. Installing system software is a system administrator function; the rest are security
administrator functions.
158 RIGHT=A
See Chapter 9. Separation of duties is used to keep “mixing up” the teams in order to prevent
situations in which two or more individuals are tempted to perform unauthorized acts.
159 RIGHT=C
See Chapter 9. Change management is the complete management function that controls changes
made to a production environment.
160 RIGHT=B
See Chapter 9. Configuration management is the support function that’s used to store version
information.
161 RIGHT=D

See Chapter 9. Configuration management is used to preserve all prior settings or versions of
software or hardware as well as to provide a “check out/check in” capability to avoid collisions.

162 RIGHT=A

See Chapter 9. Erasure is seldom 100 percent effective. Despite complex and time-consuming
methods, the slightest traces of data on media that’s been “erased” may always remain.

163 RIGHT=D

See Chapter 9. Software controls are used to protect software from unauthorized disclosure or
tampering.

164 RIGHT=B

See Chapter 9. Penetration testing is used to mimic an intruder’s activities by identifying potential
weaknesses in hardware or software.

165 RIGHT=A

See Chapter 9. Audit trails tell what happened and who did what but don’t say why.

166 RIGHT=C

See Chapter 9. The main benefit from external auditors is their objectivity. A conflict of interest is
less likely to exist when external auditors examine an information system.

167 RIGHT=B

See Chapter 9. These activities are threats. Threats describe any event that can damage or disclose
information.

168 RIGHT=C

See Chapter 9. Vulnerabilities, also known as weaknesses, are the characteristics of information
systems that can be exploited by threats.

169 RIGHT=D

See Chapter 9. A port scanner is a tool that sends out network packets in an attempt to discover
weaknesses on systems connected to the network.

170 RIGHT=C

See Chapter 9. A sniffer captures packets on the network and can store those packets for subsequent
analysis.

171 RIGHT=B

See Chapter 9. Sniffer programs perform all the same basic functions of a hardware sniffer except
that they can be installed and controlled over the network.

172 RIGHT=A

See Chapter 9. Network services such as Telnet and FTP are disabled, period, on a system in single
user mode.

173 RIGHT=D

See Chapter 9. Fraud is an activity that’s perpetrated in order to exact personal gain.

174 RIGHT=B

See Chapter 9. Denial of service is a flood of network traffic that’s intended to clog a server or
network so that it can’t service legitimate customers.

175 RIGHT=A

See Chapter 9. Intrusion detection is used to detect intrusions, attacks, and other anomalies.

176 RIGHT=C

See Chapter 9. Like anti-virus software, signature-based intrusion detection systems must be
frequently updated.

177 RIGHT=B

See Chapter 9. War driving is similar to war dialing, in which an individual with a laptop computer,
wireless LAN adaptor, and special software, can literally drive around looking for vulnerable
wireless LANs.
178 RIGHT=D
See Chapter 9. Violation processing is used to identify high levels of anomalous activity, such as the
number of unsuccessful login attempts, in order to point out possible security problems.
179 RIGHT=C
See Chapter 9. Lumens, or light level, is far less of a concern (if a concern at all) than the other
factors for the longevity of media.
180 RIGHT=A
See Chapter 9. Maintenance accounts run with privileges and features not intended for applications.
181 RIGHT=C
See Chapter 12. The primary concern here is to keep intruders out.
182 RIGHT=A
See Chapter 12. Walls that go all the way up to the ceiling do a better job of keeping fires from
spreading into or out of the data center.
183 RIGHT=A
See Chapter 12. Positive drains are those that carry liquids away from a building.
184 RIGHT=D
See Chapter 12. It’s infinitely better to find undesirable qualities such as a criminal history prior to
making an employment decision.
185 RIGHT=B
See Chapter 12. Building access systems don’t know why people are coming and going.
186 RIGHT=D
See Chapter 12. Tailgating is a common method used by someone who wants to enter a controlled
access but has no authorization for doing so.
187 RIGHT=B
Fail open refers to any controlling mechanism that remains in the “unlocked” position upon failure.
In the case of controlled building entrances, anyone will be able to enter the building. See Chapter
12.
188 RIGHT=A
See Chapter 12. Fail closed refers to any controlling mechanism that remains in the “locked”
position upon failure. In the case of controlled building entrances, no one will be able to enter the
building by normal means.
189 RIGHT=B
See Chapter 12. Wet pipe is the sprinkler system type where water is always in the pipe.
190 RIGHT=C
See Chapter 12. Preaction, a combination of dry pipe and wet pipe, is increasingly popular in data
centers.
191 RIGHT=D
See Chapter 12. Dry pipe systems take a few moments (at least) before water discharge begins.
192 RIGHT=C
See Chapter 12. Water cools the fuel to the point where the fire can’t continue.
193 RIGHT=A

See Chapter 12. Dial-up alarms don’t detect fire; they respond to a fire detector and call the fire department by using a telephone line to play a prerecorded message.

194 RIGHT=C

See Chapter 12. Signs don’t keep intruders out.

195 RIGHT=B

See Chapter 12. Guards are the most effective because they exercise judgment and make value decisions.

196 RIGHT=A

See Chapter 12. CO2 displaces oxygen long enough to stop the fire’s chemical reaction.

197 RIGHT=C

See Chapter 12. Corporations need to consider equipment removal an audit event. Having employees sign their names on a form that says they have removed thus-and-so helps to keep them honest.

198 RIGHT=B

See Chapter 12. The mantrap’s two doors are operated manually by a guard; only one door can be open at a time.

199 RIGHT=B

See Chapter 12. Eight feet is enough, which is as high as a man can jump unassisted.

200 RIGHT=D

See Chapter 12. Eight feet is too hard to climb easily, let alone mess with all that barbed wire at the top!

201 RIGHT=A

See Chapter 12. Only physical destruction will positively guarantee that the data can’t be recovered by even the most resourceful and determined persons.

202 RIGHT=C

Magnetic media must be overwritten or formatted at least seven times to ensure complete erasure.

See Chapter 12.

203 RIGHT=B

See Chapter 12. It coats the fuel so that it can no longer combine with oxygen.

204 RIGHT=D

See Chapter 12. Although media stored off-site may be useful for the other stated purposes, the primary intention is to have a set of back-up media stored in an alternate location in the event that the data center is damaged or destroyed by a natural or man-made disaster. The back-up data stored on-site, which can be used for the other stated purposes, is of no value when the data center is destroyed.

205 RIGHT=A

See Chapter 12. Some disk lock passwords don’t actually protect the disk but only prevent that particular computer from accessing it.

206 RIGHT=C

See Chapter 12. By far the data has the most potential value, possibly tens of millions of dollars or more. By comparison, the laptop costs only a few thousand dollars.

207 RIGHT=B

See Chapter 12. Audio detectors are sensitive, passive microphones. Wave pattern motion detectors emit wave patterns and note any changes in return signals, indicating moving objects. Capacitance can only detect motion a few inches in front of the detector.

208 RIGHT=A

See Chapter 12. Passive electronic cards have no batteries because they’re powered by the RF field
emitted by the reader.
209 RIGHT=B
See Chapter 12. Active electronic access cards have a power supply and aren’t powered by the
reader’s RF transmitter.
210 RIGHT=C
See Chapter 12. Cipher locks usually offer no centralized control at all.
211 RIGHT=C
See Chapter 8. Cache memory holds instructions and data that are likely to be frequently accessed.
Cache memory is faster than RAM, so it can contribute to faster performance.
212 RIGHT=A
See Chapter 8. Firmware is software that seldom changes. Firmware is generally used to control
lower-level functions in computer hardware.
213 RIGHT=B
See Chapter 8. Memory protection is a machine-level security feature that prevents one program
from being able to read or alter memory assigned to another program.
214 RIGHT=A
See Chapter 8. The virtual memory model is used to create a memory space that’s larger than the
available physical memory.
215 RIGHT=D
See Chapter 8. Open systems are those in which specifications are published and freely available,
permitting any vendor to develop components that can be used with it.
216 RIGHT=C
See Chapter 8. In a distributed architecture, information isn’t centrally stored but rather stored in a
multitude of locations. The other answers ARE security issues in distributed architectures.
217 RIGHT=B
See Chapter 8. TCB stands for Trusted Computing Base.
218 RIGHT=A
See Chapter 8. A Trusted Computing Base is the complete “big picture” of protection used in a
computer system.
219 RIGHT=B
See Chapter 8. Pipelining is the mechanism used to overlap the steps in machine instructions in order
to complete them faster.
220 RIGHT=D
FORTRAN, BASIC, and C are third-generation languages. See Chapter 8.
221 RIGHT=A
See Chapter 8. An operating system (OS) manages computer hardware and presents a consistent
interface to application programs and tools.
222 RIGHT=B
See Chapter 8. Protection rings are layers of protection domains, with the most protected domain in
the center.
223 RIGHT=A
See Chapter 8.
224 RIGHT=D
See Chapter 8. An access matrix is used to map subjects to capabilities.
225 RIGHT=B
See Chapter 8. The Bell-LaPadula model is used to control access to materials, based upon their

classification, and the classification of the individual who wishes to view them.

226 RIGHT=B

See Chapter 8. Clark-Wilson starts with a Constrained Data Item (CDI), confirms integrity state with the Integrity Verification Procedure (IVP), and changes integrity state with the Transformation Procedure (TP).

227 RIGHT=D

See Chapter 8. Some access control models are Bell-LaPadula, Take-Grant, and Access Matrix.

228 RIGHT=B

See Chapter 8. Information flow models are used to ensure that information flows in conformance to security policy.

229 RIGHT=A

See Chapter 8. The Biba Integrity Model extends the Bell-LaPadula Access Control Model into the integrity domain.

230 RIGHT=B

A Certification is the evaluation of security features according to a set of security requirements. See Chapter 8.

231 RIGHT=C

An accreditation is a formal declaration of approval for a system to perform a particular function. See Chapter 8.

232 RIGHT=C

See Chapter 8. These are all security modes, which are used to control how users can access materials depending upon their classification.

233 RIGHT=B

See Chapter 8. In a compartmented mode information system, all users have the clearance but not necessarily the authorization to access materials.

234 RIGHT=A

See Chapter 8. In a dedicated mode information system, all users have both the clearance and authorization to access information.

235 RIGHT=D

See Chapter 8. Fail closed is the property of a component that closes off all access when it fails.

236 RIGHT=C

See Chapter 8. Fail open is the property of a component that permits all access when it fails.

237 RIGHT=A

See Chapter 8. A covert channel is an unintended and unauthorized communication path.

238 RIGHT=A

See Chapter 8. Trap door is the term most often used to describe a feature that bypasses security.

239 RIGHT=B

See Chapter 8. A closed system is one that’s proprietary and for which few, if any, specifications are published.

240 RIGHT=C

See Chapter 8. Data that travels between the various components of a computer system take the bus.

241 RIGHT=A

See Chapter 5. Separation of authority makes it difficult for an individual to steal an organization’s assets because it requires others to cooperate with the would-be criminal.

242 RIGHT=C

See Chapter 5. “Open view” is the act of leaving a classified document out in the open so that it can
be viewed by anyone.
243 RIGHT=A
See Chapter 5. The information owner is ultimately responsible for the information asset and for its
initial classification.
244 RIGHT=B
See Chapter 5. The custodian protects the information on behalf of its owner.
245 RIGHT=A
See Chapter 5. Useful life, value, and age are some of the criteria used to classify information.
246 RIGHT=C
See Chapter 5. A senior management statement of security policy underscores the importance of and
support for security.
247 RIGHT=D
See Chapter 5. An advisory policy is required by the organization but is not mandated by a local or
national government.
248 RIGHT=A
A threat is a possible undesirable event that may cause harm or damage. See Chapter 5.
249 RIGHT=B
See Chapter 5. A vulnerability is a weakness that can permit an undesirable event.
250 RIGHT=A
Safeguards exist to reduce risk in some way. See Chapter 5.
251 RIGHT=D
See Chapter 5. The purpose of risk analysis is to quantify the impact of a potential threat; in other
words, to put a monetary value on the loss of information or functionality.
252 RIGHT=B
See Chapter 5. Annualized Rate of Occurrence (ARO) is a risk management term that describes the
likelihood of the occurrence of a threat.
253 RIGHT=B
See Chapter 5. Single Loss Expectancy (SLE) is the monetary value associated with an individual
threat.
254 RIGHT=B
See Chapter 5. Annualized Loss Expectancy (ALE) is the product of Single Loss Expectancy (SLE)
and Annualized Rate of Occurrence (ARO).
255 RIGHT=C
See Chapter 5. A risk analysis calculates the Annualized Loss Expectancy (ALE), which is
calculated from the value of the asset and the likelihood that one or more threats will occur.
256 RIGHT=A
See Chapter 5. The three general remedies to risk are transference, acceptance, and reduction.
257 RIGHT=D
See Chapter 5. Risk reduction refers to any measure that can be taken to reduce the risk to an asset.
258 RIGHT=A
See Chapter 5. A safeguard must meet a cost-benefit analysis, as well as be accurate and auditable.
259 RIGHT=C
Employees need to know about security policies so that they can do the right thing. See Chapter 5.
260 RIGHT=D

See Chapter 5. A “back door,” also known as a trap door, is used to circumvent security controls.
Most often they are employed to facilitate software testing, but software developers occasionally fail
to remove them.
261 RIGHT=B
See Chapter 5. Risk cannot be eliminated. “Risk mitigation” refers to the process of reducing risk to
a level that is acceptable to the organization.
262 RIGHT=A
See Chapter 5. A security guideline is a recommended action or procedure used to follow a security
policy.
263 RIGHT=C
See Chapter 5. Security standards refer to the specific products or technologies used to protect
information.
264 RIGHT=B
See Chapter 5. Private is the classification associated with personal information such as employee
salaries.
265 RIGHT=D
Security controls reduce threats and vulnerabilities. See Chapter 5.
266 RIGHT=A
See Chapter 5. Cost effectiveness generally implies re-use. In this case, using existing means for
communicating can be a cost-effective way of telling employees why security is important.
267 RIGHT=C
See Chapter 5. Information warfare is a threat that can result in undesirable actions against an
organization.
268 RIGHT=B
See Chapter 5. The three main steps to a risk analysis are the performance of quantitative and
qualitative analysis, asset valuation, and safeguard selection.
269 RIGHT=B
See Chapter 5. The PSE, or Preliminary Security Examination, is an early step performed during a
risk analysis.
270 RIGHT=D
See Chapter 5. Unclassified documents lack the sensitivity and value that classified documents
possess.
271 RIGHT=D
See Chapter 4. UDP has no guarantee of delivery, nor sequencing or acknowledgement.
272 RIGHT=B
See Chapter 4. TCP adds unnecessary overhead. Streaming video can afford to lose a packet or two.
273 RIGHT=A
See Chapter 4. Layer 1 of the OSI model is concerned only with sending and receiving bits.
274 RIGHT=A
See Chapter 4. There are four layers in the TCP/IP model: Network Access, Internet, Transport, and
Application.
275 RIGHT=B
ARP stands for Address Resolution Protocol, a method for determining which station on a LAN has
a specific IP address. See Chapter 4.
276 RIGHT=A
See Chapter 4. ARP is used to translate an IP address into a MAC address.

277 RIGHT=B
See Chapter 4. RARP is used to translate a MAC address into an IP address.
278 RIGHT=B
See Chapter 4. This is an Ipv4 address.
279 RIGHT=A
See Chapter 4. This is a MAC address.
280 RIGHT=C
See Chapter 4. Ping uses ICMP Echo Requests.
281 RIGHT=D
See Chapter 4. SMTP, or Simple Mail Transport Protocol, is used to send and receive e-mail
messages.
282 RIGHT=B
See Chapter 4. Because it encrypts and decrypts packets over the network, SSL consumes a lot of
CPU time.
283 RIGHT=D
See Chapter 4. Access control lists are used on firewalls, routers, and bastion hosts, but not on client
systems (at least not for recording passwords!).
284 RIGHT=C
See Chapter 4. Stateful inspection firewalls must capture and remember the state of each packet; this
can be very time consuming.
285 RIGHT=B
See Chapter 4. A bastion host is used to host services (such as World Wide Web and Domain Name
Services) that are accessible from the Internet.
286 RIGHT=A
See Chapter 4. NAT, or Network Address Translation, is used to convert internal “private” addresses
into public addresses.
287 RIGHT=D
See Chapter 4. Private addresses occupy three distinct ranges: 10.0.0.0 - 10.255.255.255; 172.16.0.0
- 172.31.255.255; and 192.168.0.0 - 192.168.255.255.
288 RIGHT=C
See Chapter 4. L2TP, IPSec, and PPTP are common VPN protocol standards.
289 RIGHT=B
See Chapter 4. UTP, or Unshielded Twisted Pair, is the most easily tapped type of network cable.
290 RIGHT=B
See Chapter 4. Ethernet is a BUS topology network. It is frequently wired as a star topology,
however.
291 RIGHT=A
See Chapter 4. Callback security associates a dial-in user with a callback phone number, which
requires the caller to call from a predetermined location.
292 RIGHT=C
See Chapter 4. X.25 is a packet-switched technology, as are ATM, LAPB, SMDS and VoIP.
293 RIGHT=D
See Chapter 4. FR, or Frame Relay, is a packet-switched technology.
294 RIGHT=A
See Chapter 4. PAP, or Password Authentication Protocol, uses a static password, and it is not
encrypted. It has largely been replaced by CHAP (Challenge Handshake Authentication Protocol).
295 RIGHT=C
See Chapter 4. POTS lines make it all to easy to install a rogue modem and provide an unprotected
back door to the corporate network.

296 RIGHT=A
See Chapter 4. Remote access by definition brings the corporate network to any remote location.
297 RIGHT=B
See Chapter 4. RADIUS is a remote access authentication protocol.
298 RIGHT=A
See Chapter 4. These are all encapsulation protocols, used to tunnel TCP/IP traffic.
299 RIGHT=C
See Chapter 4. Each port on a LAN switch contains traffic destined only to/from the node on that
port. No other traffic on the LAN is seen on the port.
300 RIGHT=B
See Chapter 4. Ethernet is a broadcast medium.