SSCP.exam.500q

Number: SSCP
Passing Score: 800
Time Limit: 120 min

SSCP

Systems Security Certified Practitioner

Sections

1. Access Control
2. Security Operation Adimnistration

3. Analysis and Monitoring
4. Risk, Response and Recovery
5. Cryptography
6. Network and Telecommunications

Exam A

QUESTION 1
What can be defined as a table of subjects and objects indicating what actions individual subjects can take upon individual objects?

A. A capacity table
B. An access control list
C. An access control matrix
D. A capability table

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The matrix lists the users, groups and roles down the left side and the resources and functions across the top. The cells of the matrix can either indicate that access is allowed or indicate the type of access. CBK pp 317 - 318.

AIO3, p. 169 describes it as a table if subjects and objects specifying the access rights a certain subject possesses pertaining to specific objects.
In either case, the matrix is a way of analyzing the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

"A capacity table" is incorrect.

This answer is a trap for the unwary -- it sounds a little like "capability table" but is just there to distract you.

"An access control list" is incorrect.

"It [ACL] specifies a list of users [subjects] who are allowed access to each object" CBK, p. 188 Access control lists (ACL) could be used to implement the rules identified by an access control matrix but is different from the matrix itself.

"A capability table" is incorrect.

"Capability tables are used to track, manage and apply controls based on the object and rights, or capabilities of a subject. For example, a table identifies the object, specifies access rights allowed for a subject, and permits access based on the user's posession of a capability (or ticket) for the object." CBK, pp. 191-192. To put it another way, as noted in AIO3 on p. 169, "A capabiltiy table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL."

Again, a capability table could be used to implement the rules identified by an access control matrix but is different from the matrix itself.

References:

CBK pp. 191-192, 317-318
AIO3, p. 169

QUESTION 2
Which access control model is best suited in an environment where a high security level is required and where it is desired that only the administrator grants access control?

A. DAC
B. MAC
C. Access control matrix
D. TACACS

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
MAC provides high security by regulating access based on the clearance of individual users and sensitivity labels for each object. Clearance levels and sensitivity levels cannot be modified by individual users -- for example, user Joe (SECRET clearance) cannot reclassify the "Presidential Doughnut Recipe" from "SECRET" to "CONFIDENTIAL" so that his friend Jane (CONFIDENTIAL clearance) can read it. The administrator is ultimately responsible for configuring this protection in accordance with security policy and directives from the Data Owner.

DAC is incorrect. In DAC, the data owner is responsible for controlling access to the object.

Access control matrix is incorrect. The access control matrix is a way of thinking about the access control needed by a population of subjects to a population of objects. This access control can be applied using rules, ACL's, capability tables, etc.

TACACS is incorrect. TACACS is a tool for performing user authentication.

References:
CBK, p. 187, Domain 2: Access Control.
AIO3, Chapter 4, Access Control.

QUESTION 3
Which access control model provides upper and lower bounds of access capabilities for a subject?

A. Role-based access control
B. Lattice-based access control
C. Biba access control
D. Content-dependent access control

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
In the lattice model, users are assigned security clearences and the data is classified. Access decisions are made based on the clearence of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.

The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearence of "TOP SECRET." Under Bell-LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).

Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user.

Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualiifes it as the best answer.

Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.

References:

CBK, pp. 324-325.
AIO3, pp. 291-293. See aprticularly Figure 5-19 on p. 293 for an illustration of bounds in action.

QUESTION 4
How are memory cards and smart cards different?

A. Memory cards normally hold more memory than smart cards
B. Smart cards provide a two-factor authentication whereas memory cards don't
C. Memory cards have no processing power
D. Only smart cards can be used for ATM cards

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The main difference between memory cards and smart cards is their capacity to process information. A memory card holds information but cannot process information. A smart card holds information and has the necessary hardware and software to actually process that information.

A memory card holds a user's authentication information, so that this user needs only type in a user ID or PIN and presents the memory card to the system. If the entered information and the stored information match and are approved by an authentication service, the user is successfully authenticated.

A common example of a memory card is a swipe card used to provide entry to a building. The user enters a PIN and swipes the memory card through a card reader. If this is the correct combination, the reader flashes green and the individual can open the door and enter the building.

Memory cards can also be used with computers, but they require a reader to process the information. The reader adds cost to the process, especially when one is needed for every computer. Additionally, the overhead of PIN and card generation adds additional overhead and complexity to the whole authentication process. However, a memory card provides a more secure authentication method than using only a password because the attacker would need to obtain the card and know the correct PIN.

Administrators and management need to weigh the costs and benefits of a memory card implementation as well as the security needs of the organization to determine if it is the right authentication mechanism for their environment.

One of the most prevalent weaknesses of memory cards is that data stored on the card are not protected. Unencrypted data on the card (or stored on the magnetic strip) can be extracted or copied. Unlike a smart card, where security controls and logic are embedded in the integrated circuit, memory cards do not employ an inherent mechanism to protect the data from exposure.
Very little trust can be associated with confidentiality and integrity of information on the memory cards.

The following answers are incorrect:

"Smart cards provide two-factor authentication whereas memory cards don't" is incorrect. This is not necessarily true. A memory card can be combined with a pin or password to offer two factors authentication where something you have and something you know are used for factors.

"Memory cards normally hold more memory than smart cards" is incorrect. While a memory card may or may not have more memory than a smart card, this is certainly not the best answer to the question.

"Only smart cards can be used for ATM cards" is incorrect. This depends on the decisions made by the particular institution and is not the best answer to the question.

Reference(s) used for this question:

Shon Harris, CISSP All In One, 6th edition , Access Control, Page 199 and also for people using the Kindle edition of the book you can look at Locations 46474650.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press) (Kindle Locations 2124-2139). Auerbach Publications. Kindle Edition.

QUESTION 5
Why do buffer overflows happen? What is the main cause?

A. Because buffers can only hold so much data
B. Because of improper parameter checking within the application
C. Because they are an easy weakness to exploit
D. Because of insufficient system memory

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program.

The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.

As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will not ensure that it will not cause a buffer overflow in Buffer2 of Application2.

A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:
It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.

The following are incorrect answers:
"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem - the problem is that the programmer did not check the size of the input before moving it into the buffer.

"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.

"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13319-13323). Auerbach Publications. Kindle Edition.

QUESTION 6
What is the main focus of the Bell-LaPadula security model?

A. Accountability
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The Bell-LaPadula model is a formal model dealing with confidentiality.

The Bell–LaPadula Model (abbreviated BLP) is a state machine model used for enforcing access control in government and military applications. It was developed by David Elliott Bell and Leonard J. LaPadula, subsequent to strong guidance from Roger R. Schell to formalize the U.S. Department of Defense (DoD) multilevel security (MLS) policy. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g."Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell–LaPadula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity. In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby inductively proving that the system satisfies the security objectives of the model. The Bell–LaPadula model is built on the concept of a state machine with a set of allowable states in a computer network system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy. To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The -property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The -property is also known as the Confinement property.

The Discretionary Security Property - use of an access matrix to specify the discretionary access control.

The following are incorrect answers:

Accountability is incorrect. Accountability requires that actions be traceable to the user that performed them and is not addressed by the Bell-LaPadula model.

Integrity is incorrect. Integrity is addressed in the Biba model rather than Bell-Lapadula.
Availability is incorrect. Availability is concerned with assuring that data/services are available to authorized users as specified in service level objectives and is not addressed by the Bell-Lapadula model.

References:

CBK, pp. 325-326

AIO3, pp. 279 - 284
AIOv4 Security Architecture and Design (pages 333 - 336)
AIOv5 Security Architecture and Design (pages 336 - 338)

Wikipedia at https://en.wikipedia.org/wiki/Bell-La_Padula_model

QUESTION 7
Which of the following statements pertaining to the Bell-LaPadula is TRUE if you are NOT making use of the strong star property?

A. It allows "read up."
B. It addresses covert channels.
C. It addresses management of access controls.
D. It allows "write up."

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
Bell–LaPadula Confidentiality Model10 The Bell–LaPadula model is perhaps the most well-known and significant security model, in addition to being one of the oldest models used in the creation of modern secure computing systems. Like the Trusted Computer System Evaluation Criteria (or TCSEC), it was inspired by early U.S. Department of Defense security policies and the need to prove that confidentiality could be maintained. In other words, its primary goal is to prevent disclosure as the model system moves from one state (one point in time) to another.

When the strong star property is not being used it means that both the property and the Simple Security Property rules would be applied.

The Star (*) property rule of the Bell-LaPadula model says that subjects cannot write down, this would compromise the confidentiality of the information if someone at the secret layer would write the object down to a confidential container for example.

The Simple Security Property rule states that the subject cannot read up which means that a subject at the secret layer would not be able to access objects at Top Secret for example.

You must remember: The model tells you about are NOT allowed to do. Anything else would be allowed. For example within the Bell LaPadula model you would be allowed to write up as it does not compromise the security of the information. In fact it would upgrade it to the point that you could lock yourself out of your own information if you have only a secret security clearance.

The following are incorrect answers because they are all FALSE:

"It allows read up" is incorrect. The "simple security" property forbids read up.

"It addresses covert channels" is incorrect. Covert channels are not addressed by the Bell-LaPadula model.
"It addresses management of access controls" is incorrect. Management of access controls are beyond the scope of the Bell-LaPadula model.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17595-17600). Auerbach Publications. Kindle Edition.

QUESTION 8
Which security model introduces access to objects only through programs?

A. The Biba model
B. The Bell-LaPadula model
C. The Clark-Wilson model
D. The information flow model

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
In the Clark-Wilson model, the subject no longer has direct access to objects but instead must access them through programs (well -formed transactions).
The Clark–Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.

The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.

Clark–Wilson is more clearly applicable to business and industry processes in which the integrity of the information content is paramount at any level of classification.

Integrity goals of Clark–Wilson model:

Prevent unauthorized users from making modification (Only this one is addressed by the Biba model).
Separation of duties prevents authorized users from making improper modifications.
Well formed transactions: maintain internal and external consistency i.e. it is a series of operations that are carried out to transfer the data from one consistent state to the other.

The following are incorrect answers:

The Biba model is incorrect. The Biba model is concerned with integrity and controls access to objects based on a comparison of the security level of the subject to that of the object.

The Bell-LaPdaula model is incorrect. The Bell-LaPaula model is concerned with confidentiality and controls access to objects based on a comparison of the clearence level of the subject to the classification level of the object.

The information flow model is incorrect. The information flow model uses a lattice where objects are labelled with security classes and information can flow either upward or at the same level. It is similar in framework to the Bell-LaPadula model.

References:

ISC2 Official Study Guide, Pages 325 - 327
AIO3, pp. 284 - 287
AIOv4 Security Architecture and Design (pages 338 - 342)
AIOv5 Security Architecture and Design (pages 341 - 344)
Wikipedia at: https://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 9
Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

A. The Bell-LaPadula model
B. The information flow model
C. The noninterference model
D. The Clark-Wilson model

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.

The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.
It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level.
The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.

The following are incorrect answers:

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classfication of objects and the clearences of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy.

The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subjet - interface - object).

References:

CBK, pp 325 - 326
AIO3, pp. 290 - 291
AIOv4 Security Architecture and Design (page 345) AIOv5 Security Architecture and Design (pages 347 - 348)
https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

QUESTION 10
Which of the following security models does NOT concern itself with the flow of data?

A. The information flow model
B. The Biba model
C. The Bell-LaPadula model
D. The noninterference model

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users, By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned with confidentiality and bases access control decsions on the classfication of objects and the clearences of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes.

The Biba model is incorrect. The Biba model is concerned with integrity and is a complement to the Bell-LaPadula model in that higher levels of integrity are more trusted than lower levels. Access control us based on these integrity levels to assure that read/write operations do not decrease an object's integrity.

References:

CBK, pp 325 - 326
AIO3, pp. 290 - 291

QUESTION 11
What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

A. A
B. D
C. E
D. F

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level.

A is incorrect. A or "Verified Protectection" is the highest trust level under the TCSEC.
E is incorrect. The trust levels are A - D so "E" is not a valid trust level.
F is incorrect. The trust levels are A - D so "F" is not a valid trust level.

CBK, pp. 329 - 330
AIO3, pp. 302 - 306

QUESTION 12
Which division of the Orange Book deals with discretionary protection (need-to-know)?

A. D
B. C
C. B
D. A

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
C deals with discretionary protection. See matric below:

TNI/TCSEC MATRIX

	A1	B3	B2	B1	C2	C1
DISCRETIONARY ACCESS						
Discretionary Access Control						
Identification and Authentication						
System Integrity						
System Architecture						
Security Testing						
Security Features User's Guide Trusted Facility Manual Design Documentation Test Documentation						
CONTROLLED ACCESS						
Protect Audit Trails						
Object Reuse						
MANDATORY ACCESS CONTROL						
Labels						
Mandatory Access Control						
Process isolation in system architecture						
Design Specification & Verification						
Device labels						
Subject Sensitivity Labels						
Trusted Path						
Separation of Administrator and User functions						
Covert Channel Analysis (Only Covert Storage Channel at B2)						
Trusted Facility Management						
Configuration Management						
Trusted Recovery						
Covert Channel Analysis (Both Timing and Covert Channel analysis at B3)						
Security Administrator Role Defined						
Monitor events and notify security personnel						
Trusted Distribution						
Formal Methods						
	A1	B3	B2	B1	C2	C1

TCSEC Matric

The following are incorrect answers:

D is incorrect. D deals with minimal security.
B is incorrect. B deals with mandatory protection.
A is incorrect. A deals with verified protection.
Reference(s) used for this question:
CBK, p. 329 – 330

and
Shon Harris, CISSP All In One (AIO), 6th Edition , page 392-393

QUESTION 13
Which of the following are not Remote Access concerns?

A. Justification for remote access
B. Auditing of activities
C. Regular review of access privileges
D. Access badges

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
Access badges are more relevant to physical security rather than remote access.

"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.

"Auditing of activities" is incorrect. Auditing of activites is an imporant aspect to assure that malicious or unauthorized activities are not occuring.

"Regular review of access privileges" is incorrect. Regular review of remote accept privileges is an important management responsibility.

References:
AIO3, pp. 547 - 548

QUESTION 14
Smart cards are an example of which type of control?

A. Detective control

B. Administrative control
C. Technical control
D. Physical control

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Logical or technical controls involve the restriction of access to systems and the protection of information. Smart cards and encryption are examples of these types of control.

Controls are put into place to reduce the risk an organization faces, and they come in three main flavors: administrative, technical, and physical. Administrative controls are commonly referred to as “soft controls” because they are more management-oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, as in firewalls, IDS, encryption, identification and authentication mechanisms. And physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

Many types of technical controls enable a user to access a system and the resources within that system. A technical control may be a username and password combination, a Kerberos implementation, biometrics, public key infrastructure (PKI), RADIUS, TACACS +, or authentication using a smart card through a reader connected to a system. These technologies verify the user is who he says he is by using different types of authentication methods. Once a user is properly authenticated, he can be authorized and allowed access to network resources.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 245). McGraw-Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 32).

QUESTION 15
What security model is dependent on security labels?

A. Discretionary access control
B. Label-based access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and the classification or sensitivity of the object. Label-based access control is not defined.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 16
What security model implies a central authority that define rules and sometimes global rules, dictating what subjects can have access to what objects?

A. Flow Model
B. Discretionary access control
C. Mandatory access control
D. Non-discretionary access control

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
As a security administrator you might configure user profiles so that users cannot change the system's time, alter system configuration files, access a command prompt, or install unapproved applications. This type of access control is referred to as nondiscretionary, meaning that access decisions are not made at the discretion of the user. Nondiscretionary access controls are put into place by an authoritative entity (usually a security administrator) with the goal of protecting the organization's most critical assets.

Non-discretionary access control is when a central authority determines what subjects can have access to what objects based on the organizational security policy.
Centralized access control is not an existing security model.
Both, Rule Based Access Control (RuBAC or RBAC) and Role Based Access Controls (RBAC) falls into this category.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 221). McGraw-Hill. Kindle Edition.
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 17
Which of the following access control models requires defining classification for objects?

A. Role-based access control

B. Discretionary access control C. Identity-based access control
D. Mandatory access control

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
With mandatory access control (MAC), the authorization of a subject's access to an object is dependant upon labels, which indicate the subject's clearance, and classification of objects.

The Following answers were incorrect:

Identity-based Access Control is a type of Discretionary Access Control (DAC), they are synonymous.
Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC or RBAC) are types of Non Discretionary Access Control (NDAC).

Tip:
When you have two answers that are synonymous they are not the right choice for sure.

There is only one access control model that makes use of Label, Clearances, and Categories, it is Mandatory Access Control, none of the other one makes use of those items.

Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

QUESTION 18
In the context of access control, locks, gates, guards are examples of which of the following?

A. Administrative controls
B. Technical controls
C. Physical controls
D. Logical controls

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Administrative, technical and physical controls are categories of access control mechanisms.

Logical and Technical controls are synonymous. So both of them could be eliminated as possible choices.

Physical Controls: These are controls to protect the organization's people and physical environment, such as locks, gates, and guards. Physical controls may be called "operational controls" in some contexts.

Physical security covers a broad spectrum of controls to protect the physical assets (primarily the people) in an organization. Physical Controls are sometimes referred to as "operational" controls in some risk management frameworks. These controls range from doors, locks, and windows to environment controls, construction standards, and guards. Typically, physical security is based on the notion of establishing security zones or concentric areas within a facility that require increased security as you get closer to the valuable assets inside the facility. Security zones are the physical representation of the defense-in-depth principle discussed earlier in this chapter. Typically, security zones are associated with rooms, offices, floors, or smaller elements, such as a cabinet or storage locker. The design of the physical security controls within the facility must take into account the protection of the asset as well as the individuals working in that area.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1301-1303). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1312-1318). Auerbach Publications. Kindle Edition.

QUESTION 19
Which of the following statements pertaining to using Kerberos without any extension is false?

A. A client can be impersonated by password-guessing.
B. Kerberos is mostly a third-party authentication protocol.
C. Kerberos uses public key cryptography.
D. Kerberos provides robust authentication.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.

Because a client's password is used in the initiation of the Kerberos request for the service protocol, password guessing can be used to impersonate a client.

Here is a nice overview of HOW Kerberos is implement as described in RFC 4556:

1. Introduction

The Kerberos V5 protocol [RFC4120] involves use of a trusted third party known as the Key Distribution Center (KDC) to negotiate shared session keys between clients and services and provide mutual authentication between them.

The corner-stones of Kerberos V5 are the Ticket and the Authenticator. A Ticket encapsulates a symmetric key (the ticket session key) in an envelope (a public message) intended for a specific service. The contents of the Ticket are encrypted with a symmetric key shared between the service principal and the issuing KDC. The encrypted part of the Ticket contains the client principal name, among other items. An Authenticator is a record that can be shown to have been recently generated using the ticket session key in the associated Ticket. The ticket session key is known by the client who requested the ticket. The contents of the Authenticator are encrypted with the associated ticket session key. The encrypted part of an Authenticator contains a timestamp and the client principal name, among other items.

As shown in Figure 1, below, the Kerberos V5 protocol consists of the following message exchanges between the client and the KDC, and the client and the application service:

The Authentication Service (AS) Exchange

The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT). The AS-REQ message and the ASREP message are the request and the reply message, respectively, between the client and the AS.

The Ticket Granting Service (TGS) Exchange

The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS). The TGS-REQ message and the TGS-REP message are the request and the reply message respectively between the client and the TGS.

The Client/Server Authentication Protocol (AP) Exchange

The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session-specific symmetric keys.

Usually, the AS and TGS are integrated in a single device also known as the KDC.

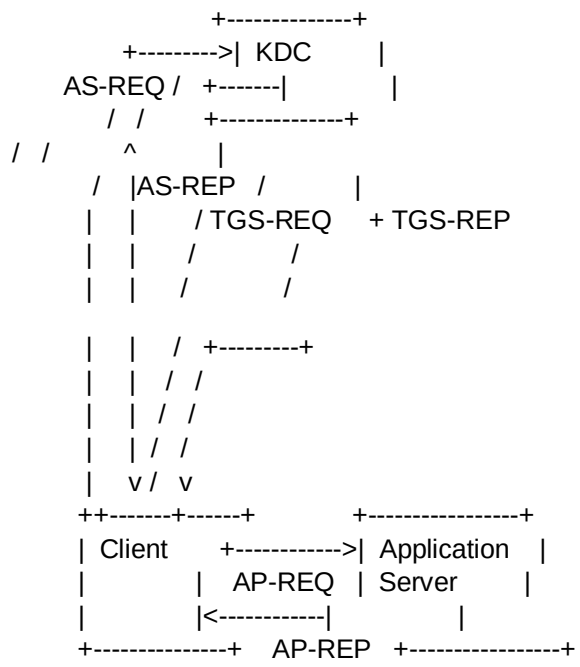


Figure 1: The Message Exchanges in the Kerberos V5 Protocol

In the AS exchange, the KDC reply contains the ticket session key, among other items, that is encrypted using a key (the AS reply key) shared between the client and the KDC. The AS reply key is typically derived from the client's password for human users. Therefore, for human users, the attack resistance strength of the Kerberos protocol is no stronger than the strength of their passwords.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 40). And
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 147-151).
and http://www.ietf.org/rfc/rfc4556.txt

QUESTION 20
Which of the following statements pertaining to Kerberos is false?

A. The Key Distribution Center represents a single point of failure.
B. Kerberos manages access permissions.
C. Kerberos uses a database to keep a copy of all users' public keys.

D. Kerberos uses symmetric key cryptography.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Kerberos is a trusted, credential-based, third-party authentication protocol that uses symmetric (secret) key cryptography to provide robust authentication to clients accessing services on a network.

One weakness of Kerberos is its Key Distribution Center (KDC), which represents a single point of failure.

The KDC contains a database that holds a copy of all of the symmetric/secret keys for the principals.

Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page40).

QUESTION 21
Which access control model would a lattice-based access control model be an example of?

A. Mandatory access control.
B. Discretionary access control.
C. Non-discretionary access control.
D. Rule-based access control.

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.

TIPS FROM CLEMENT

Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.

Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:

FIRST: The Lattice
A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.

SECOND: DAC (Discretionary Access Control)
Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control:
Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity leval and the categories the object belongs to. The categories are used to implement the Need to Know.

All of the following are forms of Non Discretionary Access Control:

Role Based Access Control (RBAC)
Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control.

In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).

The following answers are incorrect:
Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the users. It is identity based access control only. It does not make use of a lattice.

Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.

Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

References:

AIOv3 Access Control (pages 161 - 168)
AIOv3 Security Models and Architecture (pages 291 - 293)

QUESTION 22
Which of the following is an example of discretionary access control?

A. Identity-based access control

B. Task-based access control
C. Role-based access control
D. Rule-based access control

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:

An identity-based access control is an example of discretionary access control that is based on an individual's identity. Identity-based access control (IBAC) is access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Rule Based Access Control (RuBAC) and Role Based Access Control (RBAC) are examples of non-discretionary access controls.

Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.

In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action.

Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.

BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configure the proper level of access as dictated by the Data Owner.

The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.

The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.

MAC also introduce the concept of labels. Every objects will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even thou a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belong to one of the categories attached to the object.

If there is no clearance and no labels then IT IS NOT Mandatory Access Control.

Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.

DAC = Discretionary Access Control

DAC is also known as: Identity Based access control system.

The owner of an object is define as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.

Such system is good for low level of security. One of the major problem is the fact that a user who has access to someone's else file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissimination of the information.

RBAC = Role Based Access Control

RBAC is a form of Non-Discretionary access control.
Role Based access control usually maps directly with the different types of jobs performed by employees within a company.

For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.

RBAC is great tool for environment where there is a a large rotation of employees on a daily basis such as a very large help desk for example.

RBAC or RuBAC = Rule Based Access Control

RuBAC is a form of Non-Discretionary access control.

A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.
and
NISTIR-7316 at http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

and
http://itlaw.wikia.com/wiki/Identity-based_access_control

QUESTION 23
Which of the following would be used to implement Mandatory Access Control (MAC)?

A. Clark-Wilson Access Control
B. Role-based access control
C. Lattice-based access control
D. User dictated access control

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The lattice is a mechanism use to implement Mandatory Access Control (MAC)

Under Mandatory Access Control (MAC) you have:
Mandatory Access Control

Under Non Discretionary Access Control (NDAC) you have:
Rule-Based Access Control
Role-Based Access Control

Under Discretionary Access Control (DAC) you have:
Discretionary Access Control

The Lattice Based Access Control is a type of access control used to implement other access control method. A lattice is an ordered list of elements that has a least upper bound and a most lower bound. The lattice can be used for MAC, DAC, Integrity level, File Permission, and more For example in the case of MAC, if we look at common government classifications, we have the following:

TOP SECRET
SECRET ----------I am the user at secret
CONFIDENTIAL
SENSITIVE BUT UNCLASSIFIED
UNCLASSIFIED

If you look at the diagram above where I am a user at SECRET it means that I can access document at lower classification but not document at TOP SECRET. The lattice is a list of ORDERED ELEMENT, in this case the ordered elements are classification levels. My least upper bound is SECRET and my most lower bound is UNCLASSIFIED.

However the lattice could also be used for Integrity Levels such as:

VERY HIGH
HIGH
MEDIUM ----------I am a user, process, application at the medium level
LOW
VERY LOW

In the case of of Integrity levels you have to think about TRUST. Of course if I take for example the the VISTA operating system which is based on Biba then Integrity Levels would be used. As a user having access to the system I cannot tell a process running with administrative privilege what to do. Else any users on the system could take control of the system by getting highly privilege process to do things on their behalf. So no read down would be allowed in this case and this is an example of the Biba model.

Last but not least the lattice could be use for file permissions:

RWX
RW ---------User at this level
R

If I am a user with READ and WRITE (RW) access privilege then I cannot execute the file because I do not have execute permission which is the X under linux and UNIX.

Many people confuse the Lattice Model and many books says MAC = LATTICE, however the lattice can be use for other purposes.

There is also Role Based Access Control (RBAC) that exists out there. It COULD be used to simulate MAC but it is not MAC as it does not make use of Label on objects indicating sensitivity and categories. MAC also require a clearance that dominates the object.

You can get more info about RBAC at:http://csrc.nist.gov/groups/SNS/rbac/faq.html#03

Also note that many book uses the same acronym for Role Based Access Control and Rule Based Access Control which is RBAC, this can be confusing.

The proper way of writing the acronym for Rule Based Access Control is RuBAC, unfortunately it is not commonly used.

References:
There is a great article on technet that talks about the lattice in VISTA:
http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx

also see:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).
and

http://www.microsoft-watch.com/content/vista/gaging_vistas_integrity.html

QUESTION 24
Which type of attack involves impersonating a user or a system?

A. Smurfing attack

B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 25
Which of the following is NOT an advantage that TACACS+ has over TACACS?

A. Event logging
B. Use of two-factor password authentication
C. User has the ability to change his password
D. Ability for security tokens to be resynchronized

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
Although TACACS+ provides better audit trails, event logging is a service that is provided with TACACS.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 121).

QUESTION 26
Which of the following remote access authentication systems is the most robust?

A. TACACS+
B. RADIUS
C. PAP

D. TACACS

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS. PAP is not a remote access authentication system but a remote node security protocol.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 122).

QUESTION 27
Which of the following is an example of a passive attack?

A. Denying services to legitimate users
B. Shoulder surfing
C. Brute-force password cracking
D. Smurfing

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Shoulder surfing is a form of a passive attack involving stealing passwords, personal identification numbers or other confidential information by looking over someone's shoulder. All other forms of attack are active attacks, where a threat makes a modification to the system in an attempt to take advantage of a vulnerability.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 63).

QUESTION 28
What does the Clark-Wilson security model focus on?

A. Confidentiality
B. Integrity
C. Accountability
D. Availability

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 29
What does the simple security (ss) property mean in the Bell-LaPadula model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
The ss (simple security) property of the Bell-LaPadula access control model states that reading of information by a subject at a lower sensitivity level from an object at a higher sensitivity level is not permitted (no read up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).

QUESTION 30
What does the (star) property mean in the Bell-LaPadula model?

A. No write up
B. No read up
C. No write down
D. No read down

Correct Answer: C

Section: Access Control
Explanation

Explanation/Reference:
The (star) property of the Bell-LaPadula access control model states that writing of information by a subject at a higher level of sensitivity to an object at a lower level of sensitivity is not permitted (no write down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 202).
Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (page 242, 243).

QUESTION 31
What does the (star) integrity axiom mean in the Biba model?

A. No read up
B. No write down
C. No read down
D. No write up

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
The (star) integrity axiom of the Biba access control model states that an object at one level of integrity is not permitted to modify an object of a higher level of integrity (no write up).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 32
What does the simple integrity axiom mean in the Biba model?

A. No write down
B. No read down
C. No read up
D. No write up

Correct Answer: B

Section: Access Control
Explanation

Explanation/Reference:
The simple integrity axiom of the Biba access control model states that a subject at one level of integrity is not permitted to observe an object of a lower integrity (no read down).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

QUESTION 33
What is the Biba security model concerned with?

A. Confidentiality
B. Reliability
C. Availability
D. Integrity

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (Page 244).

QUESTION 34
Which security model uses division of operations into different parts and requires different users to perform each part?

A. Bell-LaPadula model
B. Biba model
C. Clark-Wilson model
D. Non-interference model

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The Clark-Wilson model uses separation of duties, which divides an operation into different parts and requires different users to perform each part. This prevents authorized users from making unauthorized modifications to data, thereby protecting its integrity.

The Clark-Wilson integrity model provides a foundation for specifying and analyzing an integrity policy for a computing system.

The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system. The model defines enforcement rules and certification rules.

The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction.

A well-formed transaction is a series of operations that transition a system from one consistent state to another consistent state.
In this model the integrity policy addresses the integrity of the transactions.
The principle of separation of duty requires that the certifier of a transaction and the implementer be different entities.

The model contains a number of basic constructs that represent both data items and processes that operate on those data items. The key data type in the ClarkWilson model is a Constrained Data Item (CDI). An Integrity Verification Procedure (IVP) ensures that all CDIs in the system are valid at a certain state. Transactions that enforce the integrity policy are represented by Transformation Procedures (TPs). A TP takes as input a CDI or Unconstrained Data Item (UDI) and produces a CDI. A TP must transition the system from one valid state to another valid state. UDIs represent system input (such as that provided by a user or adversary). A TP must guarantee (via certification) that it transforms all possible values of a UDI to a "safe" CDI.

In general, preservation of data integrity has three goals:

Prevent data modification by unauthorized parties
Prevent unauthorized data modification by authorized parties
Maintain internal and external consistency (i.e. data reflects the real world)

Clark-Wilson addresses all three rules but BIBA addresses only the first rule of intergrity.

References:
HARRIS, Shon, All-In-One CISSP Certification Fifth Edition, McGraw-Hill/Osborne, Chapter 5: Security Architecture and Design (Page 341-344).
and
http://en.wikipedia.org/wiki/Clark-Wilson_model

QUESTION 35
What is the main objective of proper separation of duties?

A. To prevent employees from disclosing sensitive information.

B. To ensure access controls are in place.
C. To ensure that no single individual can compromise a system.
D. To ensure that audit trails are not tampered with.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The primary objective of proper separation of duties is to ensure that one person acting alone cannot compromise the company's security in any way. A proper separation of duties does not prevent employees from disclosing information, nor does it ensure that access controls are in place or that audit trails are not tampered with.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 12: Operations Security (Page 808).

QUESTION 36
Which of the following is related to physical security and is not considered a technical control?

A. Access control Mechanisms
B. Intrusion Detection Systems
C. Firewalls
D. Locks

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
All of the above are considered technical controls except for locks, which are physical controls.

Administrative, Technical, and Physical Security Controls

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance, security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryptions systems, antivirus systems, firewalls, and intrusion detection systems.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control. From the GIAC.ORG website

QUESTION 37
Which of the following floors would be most appropriate to locate information processing facilities in a 6-stories building?

A. Basement
B. Ground floor
C. Third floor
D. Sixth floor

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
You data center should be located in the middle of the facility or the core of a building to provide protection from natural disasters or bombs and provide easier access to emergency crewmembers if necessary. By being at the core of the facility the external wall would act as a secondary layer of protection as well.

Information processing facilities should not be located on the top floors of buildings in case of a fire or flooding coming from the roof. Many crimes and theft have also been conducted by simply cutting a large hole on the roof.

They should not be in the basement because of flooding where water has a natural tendancy to flow down :-) Even a little amount of water would affect your operation considering the quantity of electrical cabling sitting directly on the cement floor under under your raise floor.

The data center should not be located on the first floor due to the presence of the main entrance where people are coming in and out. You have a lot of high traffic areas such as the elevators, the loading docks, cafeteria, coffee shopt, etc.. Really a bad location for a data center.

So it was easy to come up with the answer by using the process of elimination where the top, the bottom, and the basement are all bad choices. That left you with only one possible answer which is the third floor.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 5th Edition, Page 425.

QUESTION 38

Which of the following Operation Security controls is intended to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system?

A. Detective Controls
B. Preventative Controls
C. Corrective Controls
D. Directive Controls

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
In the Operations Security domain, Preventative Controls are designed to prevent unauthorized intruders from internally or externally accessing the system, and to lower the amount and impact of unintentional errors that are entering the system.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 217.

QUESTION 39
This baseline sets certain thresholds for specific errors or mistakes allowed and the amount of these occurrences that can take place before it is considered suspicious?

A. Checkpoint level
B. Ceiling level
C. Clipping level
D. Threshold level

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Organizations usually forgive a particular type, number, or pattern of violations, thus permitting a predetermined number of user errors before gathering this data for analysis. An organization attempting to track all violations, without sophisticated statistical computing ability, would be unable to manage the sheer quantity of such data. To make a violation listing effective, a clipping level must be established.

The clipping level establishes a baseline for violation activities that may be normal user errors. Only after this baseline is exceeded is a violation record produced. This solution is particularly effective for small- to medium-sized installations. Organizations with large-scale computing facilities often track all violations and use statistical routines to cull out the minor infractions (e.g., forgetting a password or mistyping it several times).

If the number of violations being tracked becomes unmanageable, the first step in correcting the problems should be to analyze why the condition has occurred. Do users understand how they are to interact with the computer resource? Are the rules too difficult to follow? Violation tracking and analysis can be valuable tools in assisting an organization to develop thorough but useable controls. Once these are in place and records are produced that accurately reflect serious violations, tracking and analysis become the first line of defense. With this procedure, intrusions are discovered before major damage occurs and sometimes early enough to catch the perpetrator. In addition, business protection and preservation are strengthened.

The following answers are incorrect:
All of the other choices presented were simply detractors.

The following reference(s) were used for this question:
Handbook of Information Security Management

QUESTION 40
Which type of control is concerned with avoiding occurrences of risks?

A. Deterrent controls
B. Detective controls
C. Preventive controls
D. Compensating controls

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Preventive controls are concerned with avoiding occurrences of risks while deterrent controls are concerned with discouraging violations. Detecting controls identify occurrences and compensating controls are alternative controls, used to compensate weaknesses in other controls. Supervision is an example of compensating control.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 41
Which type of control is concerned with restoring controls?

A. Compensating controls
B. Corrective controls
C. Detective controls
D. Preventive controls

Correct Answer: B
Section: Access Control
Explanation
Explanation/Reference:
Corrective controls are concerned with remedying circumstances and restoring controls.

Detective controls are concerned with investigating what happen after the fact such as logs and video surveillance tapes for example.

Compensating controls are alternative controls, used to compensate weaknesses in other controls.
Preventive controls are concerned with avoiding occurrences of risks.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 42
Which of the following biometric parameters are better suited for authentication use over a long period of time?

A. Iris pattern
B. Voice pattern
C. Signature dynamics
D. Retina pattern

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
The iris pattern is considered lifelong. Unique features of the iris are: freckles, rings, rifts, pits, striations, fibers, filaments, furrows, vasculature and coronas. Voice, signature and retina patterns are more likely to change over time, thus are not as suitable for authentication over a long period of time without needing reenrollment.

Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 1 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

QUESTION 43
In the CIA triad, what does the letter A stand for?

A. Auditability
B. Accountability
C. Availability
D. Authentication

Correct Answer: C
Section: Access Control
Explanation
Explanation/Reference:
The CIA triad stands for Confidentiality, Integrity and Availability.

QUESTION 44
Which TCSEC class specifies discretionary protection?

A. B2
B. B1
C. C2
D. C1

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
C1 involves discretionary protection, C2 involves controlled access protection, B1 involves labeled security protection and B2 involves structured protection.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 45
Which of the following access control techniques best gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure?

A. Access control lists

B. Discretionary access control
C. Role-based access control
D. Non-mandatory access control

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Role-based access control (RBAC) gives the security officers the ability to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. Each user is assigned one or more roles, and each role is assigned one or more privileges that are given to users in that role. An access control list (ACL) is a table that tells a system which access rights each user has to a particular system object. With discretionary access control, administration is decentralized and owners of resources control other users' access. Non-mandatory access control is not a defined access control technique.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 9).

QUESTION 46
Which access control model was proposed for enforcing access control in government and military applications?

A. Bell-LaPadula model
B. Biba model
C. Sutherland model
D. Brewer-Nash model

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
The Bell-LaPadula model, mostly concerned with confidentiality, was proposed for enforcing access control in government and military applications. It supports mandatory access control by determining the access rights from the security levels associated with subjects and objects. It also supports discretionary access control by checking access rights from an access matrix. The Biba model, introduced in 1977, the Sutherland model, published in 1986, and the Brewer-Nash model, published in 1989, are concerned with integrity.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 2: Access Control Systems and Methodology (page 11).

QUESTION 47
Which of the following biometric devices has the lowest user acceptance level?

A. Retina Scan

B. Fingerprint scan
C. Hand geometry
D. Signature recognition

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
According to the cited reference, of the given options, the Retina scan has the lowest user acceptance level as it is needed for the user to get his eye close to a device and it is not user friendly and very intrusive.

However, retina scan is the most precise with about one error per 10 millions usage.

Look at the 2 tables below. If necessary right click on the image and save it on your desktop for a larger view or visit the web site directly at https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy .
Biometric Comparison Chart

BIOMETRICS COMPARISON CHART

Biometric	Verify	ID	Accuracy	Reliability	Error Rate	Errors	False Pos.	False Neg.
Fingerprint	Yes	Yes	Very High	High	1 in 500+	dryness, dirt, age	Ext. Diff.	Ext. Diff.
Facial Recognition	Yes	No	High	Medium	no data	lighting, age, glasses, hair	Difficult	Easy
Hand Geometry	Yes	No	High	Medium	1 in 500	hand injury, age	Very Diff.	Medium
Speaker Recognition	Yes	No	Medium	Low	1 in 50	noise, weather, colds	Medium	Easy
Iris Scan	Yes	Yes	Very High	High	1 in 131,000	poor lighting	Very Diff.	Very Diff.
Retinal Scan	Yes	Yes	Very High	High	1 in 10,000,000	glasses	Ext. Diff.	Ext. Diff.
Signature Recognition	Yes	No	Medium	Low	1 in 50	changing signatures	Medium	Easy
Keystroke Recognition	Yes	No	Low	Low	no data	hand injury, tiredness	Difficult	Easy
DNA	Yes	Yes	Very High	High	no data	none	Ext. Diff.	Ext. Diff.

Biometric	Security Level	Long-term Stability	User Acceptance	Intrusive	Ease of Use	Low Cost	Hardware	Standards
Fingerprint	High	High	Medium	Somewhat	High	Yes	Special, cheap	Yes
Facial Recognition	Medium	Medium	Medium	Non	Medium	Yes	Common, cheap	?
Hand Geometry	Medium	Medium	Medium	Non	High	No	Special, mid-price	?
Speaker Recognition	Medium	Medium	High	Non	High	Yes	Common, cheap	?
Iris Scan	High	High	Medium	Non	Medium	No	Special, expensive	?
Retinal Scan	High	High	Medium	Very	Low	No	Special, expensive	?
Signature Recognition	Medium	Medium	Medium	Non	High	Yes	Special, mid-price	?
Keystroke Recognition	Medium	Low	High	Non	High	Yes	Common, cheap	?
DNA	High	High	Low	Extremely	Low	No	Special, expensive	Yes

Aspect descriptions:

Verify Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be.

ID Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many peopleto see which person the user is.

Accuracy How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.

Reliability How dependable the Biometric is for recognition purposes.

Error Rate This is calculated as the crossing point when graphed of false positives and false negatives created using this Biometric.

Errors Typical causes of errors for this Biometric.

False Pos. How easy it is to create a false positive reading with this biometric (someone is able to impersonate someone else).

False Neg. How easy it is to create a false negative reading with this biometric (someone is able to avoid identification as oneself).

Security Level The highest level of security that this Biometric is capable of working at.

Long-term Stability How well this Biometric continues to work without data updates over long periods of time.

User Acceptance How willing the public is to use this Biometric.

Intrusiveness How much the Biometric is considered to invade one's privacy or require interaction by the user.

Ease of Use How easy this Biometric is for both the user and the personnel involved.

Low Cost Whether or not there is a low-cost option for this Biometric to be used.

Hardware Type and cost of hardware required to use this Biometric.

Standards Whether or not standards exist for this Biometric.

Biometric Aspect Descriptions

Reference(s) used for this question:

RHODES, Keith A., Chief Technologist, United States General Accounting Office, National Preparedness, Technologies to Secure Federal Buildings, April 2002 (page 10).

and
https://sites.google.com/site/biometricsecuritysolutions/crossover-accuracy

QUESTION 48
Which of the following would be an example of the best password?

A. golf001
B. Elizabeth
C. T1me4g0lF
D. password

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The best passwords are those that are both easy to remember and hard to crack using a dictionary attack. The best way to create passwords that fulfil both criteria is to use two small unrelated words or phonemes, ideally with upper and lower case characters, a special character, and/or a number. Shouldn't be used: common names, DOB, spouse, phone numbers, words found in dictionaries or system defaults. Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 1.

QUESTION 49
A network-based vulnerability assessment is a type of test also referred to as:

A. An active vulnerability assessment.
B. A routing vulnerability assessment.
C. A host-based vulnerability assessment.
D. A passive vulnerability assessment.

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
A network-based vulnerability assessment tool/system either re-enacts system attacks, noting and recording responses to the attacks, or probes different targets to infer weaknesses from their responses.

Since the assessment is actively attacking or scanning targeted systems, network-based vulnerability assessment systems are also called active vulnerability systems.

There are mostly two main types of test:

PASSIVE: You don't send any packet or interact with the remote target. You make use of public database and other techniques to gather information about your target.

ACTIVE: You do send packets to your target, you attempt to stimulate response which will help you in gathering information about hosts that are alive, services runnings, port state, and more.

See example below of both types of attacks:
Eavesdropping and sniffing data as it passes over a network are considered passive attacks because the attacker is not affecting the protocol, algorithm, key, message, or any parts of the encryption system. Passive attacks are hard to detect, so in most cases methods are put in place to try to prevent them rather than to detect and stop them.

Altering messages , modifying system files, and masquerading as another individual are acts that are considered active attacks because the attacker is actually doing something instead of sitting back and gathering data. Passive attacks are usually used to gain information prior to carrying out an active attack.

IMPORTANT NOTE:
On the commercial vendors will sometimes use different names for different types of scans. However, the exam is product agnostic. They do not use vendor terms but general terms. Experience could trick you into selecting the wrong choice sometimes. See feedback from Jason below:

"I am a system security analyst. It is my daily duty to perform system vulnerability analysis. We use Nessus and Retina (among other tools) to perform our network based vulnerability scanning. Both commercially available tools refer to a network based vulnerability scan as a "credentialed" scan. Without credentials, the scan tool cannot login to the system being scanned, and as such will only receive a port scan to see what ports are open and exploitable"

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 865). McGraw-Hill. Kindle Edition.
and
DUPUIS, Clement, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0, march 2002 (page 97).

QUESTION 50
Which of the following is NOT a form of detective administrative control?

A. Rotation of duties
B. Required vacations
C. Separation of duties

D. Security reviews and audits

Correct Answer: C
Section: Access Control
Explanation
Explanation/Reference:
Detective administrative controls warn of administrative control violations. Rotation of duties, required vacations and security reviews and audits are forms of detective administrative controls. Separation of duties is the practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process, thus a preventive control rather than a detective control.
Source: DUPUIS, Cl?ment, Access Control Systems and Methodology CISSP Open Study Guide, version 1.0 (march 2002).

QUESTION 51
Which TCSEC level is labeled Controlled Access Protection?

A. C1 B.
C2
C. C3
D. B1

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
C2 is labeled Controlled Access Protection.

The TCSEC defines four divisions: D, C, B and A where division A has the highest security.

Each division represents a significant difference in the trust an individual or organization can place on the evaluated system. Additionally divisions C, B and A are broken into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1.

Each division and class expands or modifies as indicated the requirements of the immediately prior division or class.
D — Minimal protection

Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher division

C — Discretionary protection

C1 — Discretionary Security Protection

Identification and authentication
Separation of users and data
Discretionary Access Control (DAC) capable of enforcing access limitations on an individual basis
Required System Documentation and user manuals
C2 — Controlled Access Protection
More finely grained DAC

Individual accountability through login procedures
Audit trails
Object reuse
Resource isolation

B — Mandatory protection

B1 — Labeled Security Protection
Informal statement of the security policy model
Data sensitivity labels
Mandatory Access Control (MAC) over selected subjects and objects
Label exportation capabilities
All discovered flaws must be removed or otherwise mitigated
Design specifications and verification
B2 — Structured Protection
Security policy model clearly defined and formally documented
DAC and MAC enforcement extended to all subjects and objects
Covert storage channels are analyzed for occurrence and bandwidth
Carefully structured into protection-critical and non-protection-critical elements
Design and implementation enable more comprehensive testing and review
Authentication mechanisms are strengthened
Trusted facility management is provided with administrator and operator segregation
Strict configuration management controls are imposed
B3 — Security Domains
Satisfies reference monitor requirements
Structured to exclude code not essential to security policy enforcement
Significant system engineering directed toward minimizing complexity
Security administrator role defined
Audit security-relevant events
Automated imminent intrusion detection, notification, and response
Trusted system recovery procedures

Covert timing channels are analyzed for occurrence and bandwidth
An example of such a system is the XTS-300, a precursor to the XTS-400

A — Verified protection

A1 — Verified Design
Functionally identical to B3
Formal design and verification techniques including a formal top-level specification
Formal management and distribution procedures
An example of such a system is Honeywell's Secure Communications Processor SCOMP, a precursor to the XTS-400
Beyond A1

System Architecture demonstrates that the requirements of self-protection and completeness for reference monitors have been implemented in the Trusted Computing Base (TCB).
Security Testing automatically generates test-case from the formal top-level specification or formal lower-level specifications.
Formal Specification and Verification is where the TCB is verified down to the source code level, using formal verification methods where feasible.
Trusted Design Environment is where the TCB is designed in a trusted facility with only trusted (cleared) personnel.

The following are incorrect answers:

C1 is Discretionary security
C3 does not exists, it is only a detractor
B1 is called Labeled Security Protection.

Reference(s) used for this question:

HARE, Chris, Security management Practices CISSP Open Study Guide, version 1.0, april 1999.

and
AIOv4 Security Architecture and Design (pages 357 - 361)
AIOv5 Security Architecture and Design (pages 358 - 362)

QUESTION 52
Which security model is based on the military classification of data and people with clearances?

A. Brewer-Nash model
B. Clark-Wilson model
C. Bell-LaPadula model

D. Biba model

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The Bell-LaPadula model is a confidentiality model for information security based on the military classification of data, on people with clearances and data with a classification or sensitivity model. The Biba, Clark-Wilson and Brewer-Nash models are concerned with integrity. Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 53
What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

A. Central station alarm
B. Proprietary alarm
C. A remote station alarm
D. An auxiliary station alarm

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.

Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.

Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vincinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.

A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.

A remote system differs from an auxiliary system in that it does not use the municipal fire of police alarm circuits.

Reference(s) used for this question:

ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).
and
Great presentation J.T.A. Stone on SlideShare

QUESTION 54
Which of the following does not apply to system-generated passwords?

A. Passwords are harder to remember for users.
B. If the password-generating algorithm gets to be known, the entire system is in jeopardy.
C. Passwords are more vulnerable to brute force and dictionary attacks.
D. Passwords are harder to guess for attackers.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Users tend to choose easier to remember passwords. System-generated passwords can provide stronger, harder to guess passwords. Since they are based on rules provided by the administrator, they can include combinations of uppercase/lowercase letters, numbers and special characters, making them less vulnerable to brute force and dictionary attacks. One danger is that they are also harder to remember for users, who will tend to write them down, making them more vulnerable to anyone having access to the user's desk. Another danger with system-generated passwords is that if the password-generating algorithm gets to be known, the entire system is in jeopardy.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 64).

QUESTION 55
Which of the following is not a preventive login control?

A. Last login message
B. Password aging
C. Minimum password length

D. Account expiration

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
The last login message displays the last login date and time, allowing a user to discover if their account was used by someone else. Hence, this is rather a detective control.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 63).

QUESTION 56
Which of the following forms of authentication would most likely apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier?

A. Dynamic authentication
B. Continuous authentication
C. Encrypted authentication
D. Robust authentication

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.
Source: GUTTMAN, Barbara & BAGWILL, Robert, NIST Special Publication 800-xx, Internet Security Policy: A Technical Guide, Draft Version, May 25, 2000 (page 34).

QUESTION 57
Who first described the DoD multilevel military security policy in abstract, formal terms?

A. David Bell and Leonard LaPadula

B. Rivest, Shamir and Adleman
C. Whitfield Diffie and Martin Hellman
D. David Clark and David Wilson

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
It was David Bell and Leonard LaPadula who, in 1973, first described the DoD multilevel military security policy in abstract, formal terms. The Bell-LaPadula is a Mandatory Access Control (MAC) model concerned with confidentiality. Rivest, Shamir and Adleman (RSA) developed the RSA encryption algorithm. Whitfield Diffie and Martin Hellman published the Diffie-Hellman key agreement algorithm in 1976. David Clark and David Wilson developed the Clark-Wilson integrity model, more appropriate for security in commercial activities.
Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (pages 78,109).

QUESTION 58
What is the most critical characteristic of a biometric identifying system?

A. Perceived intrusiveness
B. Storage requirements

C. Accuracy D. Scalability

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Accuracy is the most critical characteristic of a biometric identifying verification system.

Accuracy is measured in terms of false rejection rate (FRR, or type I errors) and false acceptance rate (FAR or type II errors).

The Crossover Error Rate (CER) is the point at which the FRR equals the FAR and has become the most important measure of biometric system accuracy.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 9).

QUESTION 59
What is considered the most important type of error to avoid for a biometric access control system?

A. Type I Error
B. Type II Error
C. Combined Error Rate
D. Crossover Error Rate

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
When a biometric system is used for access control, the most important error is the false accept or false acceptance rate, or Type II error, where the system would accept an impostor.

A Type I error is known as the false reject or false rejection rate and is not as important in the security context as a type II error rate. A type one is when a valid company employee is rejected by the system and he cannot get access even thou it is a valid user.

The Crossover Error Rate (CER) is the point at which the false rejection rate equals the false acceptance rate if your would create a graph of Type I and Type II errors. The lower the CER the better the device would be.

The Combined Error Rate is a distracter and does not exist.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 1, Biometric Identification (page 10).

QUESTION 60
How can an individual/person best be identified or authenticated to prevent local masquarading attacks?

A. UserId and password

B. Smart card and PIN code
C. Two-factor authentication
D. Biometrics

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification). Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.

Some people are getting thrown off by the term Masquarade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.

A UserId only provides for identification.

A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.

A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.

Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.

I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.

I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.

The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes.

Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification.

There are always THREE means of authentication, they are:

Something you know (Type 1)
Something you have (Type 2)
Something you are (Type 3)

Reference(s) used for this question:
TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7).
and

Search Security at http://searchsecurity.techtarget.com/definition/masquerade

QUESTION 61
Which authentication technique best protects against hijacking?

A. Static authentication
B. Continuous authentication
C. Robust authentication

D. Strong authentication

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
A continuous authentication provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. This is the best protection against hijacking. Static authentication is the type of authentication provided by traditional password schemes and the strength of the authentication is highly dependent on the difficulty of guessing passwords. The robust authentication mechanism relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, and it does not protect against hijacking. Strong authentication refers to a two-factor authentication (like something a user knows and something a user is).
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3: Secured Connections to External Networks (page 51).

QUESTION 62
Which of the following is not a security goal for remote access?

A. Reliable authentication of users and systems
B. Protection of confidential data
C. Easy to manage access control to systems and network resources
D. Automated login for remote users

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
An automated login function for remote users would imply a weak authentication, thus certainly not a security goal.
Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition, volume 2, 2001, CRC Press, Chapter 5: An Introduction to Secure Remote Access (page 100).

QUESTION 63
Which of the following questions is less likely to help in assessing identification and authentication controls?

A. Is a current list maintained and approved of authorized users and their access?
B. Are passwords changed at least every ninety days or earlier if needed?
C. Are inactive user identifications disabled after a specified period of time?

D. Is there a process for reporting incidents?

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
Identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. Reporting incidents is more related to incident response capability (operational control) than to identification and authentication (technical control).
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A30 to A-32).

QUESTION 64
Which of the following questions is less likely to help in assessing physical access controls?

A. Does management regularly review the list of persons with physical access to sensitive facilities?
B. Is the operating system configured to prevent circumvention of the security software and application controls?
C. Are keys or other access devices needed to enter the computer room and media library?
D. Are visitors to sensitive areas signed in and escorted?

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical access controls except for the one regarding operating system configuration, which is a logical access control.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A21 to A-24).

QUESTION 65
Which of the following questions is less likely to help in assessing physical and environmental protection?

A. Are entry codes changed periodically?
B. Are appropriate fire suppression and prevention devices installed and working?
C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?

D. Is physical access to data transmission lines controlled?

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control.
Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A21 to A-24).

QUESTION 66
How would nonrepudiation be best classified as?

A. A preventive control
B. A logical control
C. A corrective control
D. A compensating control

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
Systems accountability depends on the ability to ensure that senders cannot deny sending information and that receivers cannot deny receiving it. Because the mechanisms implemented in nonrepudiation prevent the ability to successfully repudiate an action, it can be considered as a preventive control.
Source: STONEBURNER, Gary, NIST Special Publication 800-33: Underlying Technical Models for Information Technology Security, National Institute of Standards and Technology, December 2001, page 7.

QUESTION 67
Why should batch files and scripts be stored in a protected area?

A. Because of the least privilege concept.

B. Because they cannot be accessed by operators.

C. Because they may contain credentials.D. Because of the need-to-know concept.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Because scripts contain credentials, they must be stored in a protected area and the transmission of the scripts must be dealt with carefully. Operators might need access to batch files and scripts. The least privilege concept requires that each subject in a system be granted the most restrictive set of privileges needed for the performance of authorized tasks. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

QUESTION 68
Which of the following Kerberos components holds all users' and services' cryptographic keys?

A. The Key Distribution Service
B. The Authentication Service
C. The Key Distribution Center
D. The Key Granting Service

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The Key Distribution Center (KDC) holds all users' and services' cryptographic keys. It provides authentication services, as well as key distribution functionality. The Authentication Service is the part of the KDC that authenticates a principal. The Key Distribution Service and Key Granting Service are distracters and are not defined Kerberos components.
Source: WALLHOFF, John, CISSP Summary 2002, April 2002, CBK#1 Access Control System & Methodology (page 3)

QUESTION 69
Sensitivity labels are an example of what application control type?

A. Preventive security controls
B. Detective security controls
C. Compensating administrative controls

D. Preventive accuracy controls

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
Sensitivity labels are a preventive security application controls, such as are firewalls, reference monitors, traffic padding, encryption, data classification, one-time passwords, contingency planning, separation of development, application and test environments.

The incorrect answers are:

Detective security controls - Intrusion detection systems (IDS), monitoring activities, and audit trails.

Compensating administrative controls - There no such application control.

Preventive accuracy controls - data checks, forms, custom screens, validity checks, contingency planning, and backups.

Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 264).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Application Controls, Figure 7.1 (page 360).

QUESTION 70
Which integrity model defines a constrained data item, an integrity verification procedure and a transformation procedure?

A. The Take-Grant model
B. The Biba integrity model
C. The Clark Wilson integrity model
D. The Bell-LaPadula integrity model

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The Clark Wilson integrity model addresses the three following integrity goals: 1) data is protected from modification by unauthorized users; 2) data is protected from unauthorized modification by authorized users; and 3) data is internally and externally consistent. It also defines a Constrained Data Item (CDI), an Integrity

Verification Procedure (IVP), a Transformation Procedure (TP) and an Unconstrained Data item. The Bell-LaPadula and Take-Grant models are not integrity models.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5:

Security Architecture and Models (page 205).

QUESTION 71
How should a doorway of a manned facility with automatic locks be configured?

A. It should be configured to be fail-secure.
B. It should be configured to be fail-safe.
C. It should have a door delay cipher lock.
D. It should not allow piggybacking.

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Access controls are meant to protect facilities and computers as well as people.

In some situations, the objectives of physical access controls and the protection of people's lives may come into conflict. In theses situations, a person's life always takes precedence.

Many physical security controls make entry into and out of a facility hard, if not impossible. However, special consideration needs to be taken when this could affect lives. In an information processing facility, different types of locks can be used and piggybacking should be prevented, but the issue here with automatic locks is that they can either be configured as fail-safe or fail-secure.

Since there should only be one access door to an information processing facility, the automatic lock to the only door to a man-operated room must be configured to allow people out in case of emergency, hence to be fail-safe (sometimes called fail-open), meaning that upon fire alarm activation or electric power failure, the locking device unlocks. This is because the solenoid that maintains power to the lock to keep it in a locked state fails and thus opens or unlocks the electronic lock.

Fail Secure works just the other way. The lock device is in a locked or secure state with no power applied. Upon authorized entry, a solinoid unlocks the lock temporarily. Thus in a Fail Secure lock, loss of power of fire alarm activation causes the lock to remain in a secure mode.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 451). McGraw-Hill. Kindle Edition.
and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20249-20251). Auerbach Publications. Kindle Edition.

QUESTION 72
Which of following is not a service provided by AAA servers (Radius, TACACS and DIAMETER)?

A. Authentication
B. Administration
C. Accounting
D. Authorization

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Radius, TACACS and DIAMETER are classified as authentication, authorization, and accounting (AAA) servers.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

also see:
The term "AAA" is often used, describing cornerstone concepts [of the AIC triad] Authentication, Authorization, and Accountability. Left out of the AAA acronym is Identification which is required before the three "A's" can follow. Identity is a claim, Authentication proves an identity, Authorization describes the action you can perform on a system once you have been identified and authenticated, and accountability holds users accountable for their actions. Reference: CISSP Study Guide, Conrad Misenar, Feldman p. 10-11, (c) 2010 Elsevier.

QUESTION 73
In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

A. Access-Accept
B. Access-Reject
C. Access-Granted
D. Access-Challenge

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:

In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

QUESTION 74
Which of the following statements pertaining to RADIUS is incorrect:

A. A RADIUS server can act as a proxy server, forwarding client requests to other authentication domains.
B. Most of RADIUS clients have a capability to query secondary RADIUS servers for redundancy.
C. Most RADIUS servers have built-in database connectivity for billing and reporting purposes.
D. Most RADIUS servers can work with DIAMETER servers.

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
This is the correct answer because it is FALSE.

Diameter is an AAA protocol, AAA stands for authentication, authorization and accounting protocol for computer networks, and it is a successor to RADIUS.

The name is a pun on the RADIUS protocol, which is the predecessor (a diameter is twice the radius).

The main differences are as follows:

Reliable transport protocols (TCP or SCTP, not UDP)
The IETF is in the process of standardizing TCP Transport for RADIUS
Network or transport layer security (IPsec or TLS)
The IETF is in the process of standardizing Transport Layer Security for RADIUS
Transition support for RADIUS, although Diameter is not fully compatible with RADIUS
Larger address space for attribute-value pairs (AVPs) and identifiers (32 bits instead of 8 bits)
Client–server protocol, with exception of supporting some server-initiated messages as well
Both stateful and stateless models can be used
Dynamic discovery of peers (using DNS SRV and NAPTR)
Capability negotiation
Supports application layer acknowledgements, defines failover methods and state machines (RFC 3539)
Error notification
Better roaming support

More easily extended; new commands and attributes can be defined
Aligned on 32-bit boundaries
Basic support for user-sessions and accounting

A Diameter Application is not a software application, but a protocol based on the Diameter base protocol (defined in RFC 3588). Each application is defined by an application identifier and can add new command codes and/or new mandatory AVPs. Adding a new optional AVP does not require a new application.

Examples of Diameter applications:

Diameter Mobile IPv4 Application (MobileIP, RFC 4004)

Diameter Network Access Server Application (NASREQ, RFC 4005)
Diameter Extensible Authentication Protocol (EAP) Application (RFC 4072)
Diameter Credit-Control Application (DCCA, RFC 4006)
Diameter Session Initiation Protocol Application (RFC 4740)
Various applications in the 3GPP IP Multimedia Subsystem

All of the other choices presented are true. So Diameter is backwork compatible with Radius (to some extent) but the opposite is false.

Reference(s) used for this question:

TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 38.
and
https://secure.wikimedia.org/wikipedia/en/wiki/Diameter_%28protocol%29

QUESTION 75
Which of the following is used by RADIUS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

QUESTION 76
Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

A. TCP
B. SSL
C. UDP
D. SSH

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP.

TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.
TACACS+

TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP). Since TCP is connection oriented protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless.

RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.

Reference(s) used for this question:
http://en.wikipedia.org/wiki/TACACS
and

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw-Hill. Kindle Edition.

QUESTION 77
Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

A. Using a TACACS+ server.
B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
C. Setting modem ring count to at least 5.
D. Only attaching modems to non-networked hosts.

Correct Answer: B
Section: Access Control
Explanation
Explanation/Reference:
Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.

The use of a TACACS+ Server by itself cannot eliminate hacking.

Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.

Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.
Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

QUESTION 78
In the Bell-LaPadula model, the Star-property is also called:

A. The simple security property
B. The confidentiality property
C. The confinement property
D. The tranquility property

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:

The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.

In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.

The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.

To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.

The Discretionary Security Property - use an access control matrix to specify the discretionary access control.

The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.

Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.

With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).
Strong Property

The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.

Tranquility principle

The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.

Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.

Reference(s) used for this question:
http://en.wikipedia.org/wiki/Biba_Model
http://en.wikipedia.org/wiki/Mandatory_access_control
http://en.wikipedia.org/wiki/Discretionary_access_control
http://en.wikipedia.org/wiki/Clark-Wilson_model
http://en.wikipedia.org/wiki/Brewer_and_Nash_model

QUESTION 79
An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

A. active attack
B. outside attack
C. inside attack
D. passive attack

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 80

Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

A. Extensible Authentication Protocol
B. Challenge Handshake Authentication ProtocolC. Remote Authentication Dial-In User Service
D. Multilevel Authentication Protocol.

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 81
What is a common problem when using vibration detection devices for perimeter control?

A. They are vulnerable to non-adversarial disturbances.
B. They can be defeated by electronic means.
C. Signal amplitude is affected by weather conditions.
D. They must be buried below the frost line.

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
Vibration sensors are similar and are also implemented to detect forced entry. Financial institutions may choose to implement these types of sensors on exterior walls, where bank robbers may attempt to drive a vehicle through. They are also commonly used around the ceiling and flooring of vaults to detect someone trying to make an unauthorized bank withdrawal.

Such sensors are proned to false positive. If there is a large truck with heavy equipment driving by it may trigger the sensor. The same with a storm with thunder and lighting, it may trigger the alarm even thou there are no adversarial threat or disturbance.

The following are incorrect answers:

All of the other choices are incorrect.

Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (pp. 495-496). McGraw-Hill . Kindle Edition.

QUESTION 82
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Section: Access Control
Explanation

Explanation/Reference:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.

Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 83
What is the name of the first mathematical model of a multi-level security policy used to define the concept of a secure state, the modes of access, and rules for granting access?

A. Clark and Wilson Model
B. Harrison-Ruzzo-Ullman Model
C. Rivest and Shamir Model
D. Bell-LaPadula Model

Correct Answer: D
Section: Access Control
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 84
Which of the following models does NOT include data integrity or conflict of interest?

A. Biba
B. Clark-Wilson
C. Bell-LaPadula
D. Brewer-Nash

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:

Bell LaPadula model (Bell 1975): The granularity of objects and subjects is not predefined, but the model prescribes simple access rights. Based on simple access restrictions the Bell LaPadula model enforces a discretionary access control policy enhanced with mandatory rules. Applications with rigid confidentiality requirements and without strong integrity requirements may properly be modeled.

These simple rights combined with the mandatory rules of the policy considerably restrict the spectrum of applications which can be appropriately modeled.
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

Also check:
Proceedings of the IFIP TC11 12th International Conference on Information Security, Samos (Greece), May 1996, On Security Models.

QUESTION 85
What is the PRIMARY use of a password?

A. Allow access to files.
B. Identify the user.
C. Authenticate the user.
D. Segregate various user's accesses.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 86
The three classic ways of authenticating yourself to the computer security software are: something you know, something you have, and something:

A. you need.
B. you read.
C. you are.
D. you do.

Correct Answer: C
Section: Access Control
Explanation

Explanation/Reference:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 87
An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

A. Discretionary Access
B. Least Privilege
C. Mandatory Access
D. Separation of Duties

Correct Answer: B
Section: Access Control
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 88
When backing up an applications system's data, which of the following is a key question to be answered first?

A. When to make backups
B. Where to keep backups
C. What records to backup
D. How to store backups

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
It is critical that a determination be made of WHAT data is important and should be retained and protected. Without determining the data to be backed up, the potential for error increases. A record or file could be vital and yet not included in a backup routine. Alternatively, temporary or insignificant files could be included in a backup routine unnecessarily.

The following answers were incorrect:

When to make backups Although it is important to consider schedules for backups, this is done after the decisions are made of what should be included in the backup routine.

Where to keep backups The location of storing backup copies of data (Such as tapes, on-line backups, etc) should be made after determining what should be included in the backup routine and the method to store the backup.

How to store backups The backup methodology should be considered after determining what data should be included in the backup routine.

QUESTION 89
A 'Pseudo flaw' is which of the following?

A. An apparent loophole deliberately implanted in an operating system program as a trap for intruders.
B. An omission when generating Psuedo-code.
C. Used for testing for bounds violations in application programming.
D. A normally generated page fault causing the system to halt.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A Pseudo flaw is something that looks like it is vulnerable to attack, but really acts as an alarm or triggers automatic actions when an intruder attempts to exploit the flaw.

The following answers are incorrect:

An omission when generating Psuedo-code. Is incorrect because it is a distractor.
Used for testing for bounds violations in application programming. Is incorrect, this is a testing methodology.
A normally generated page fault causing the system to halt. This is incorrect because it is distractor.

QUESTION 90
Which of the following is considered the weakest link in a security system?

A. People
B. Software
C. Communications
D. Hardware

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Answer: People. The other choices can be strengthened and counted on (For the most part) to remain consistent if properly protected. People are fallible and unpredictable. Most security intrusions are caused by employees. People get tired, careless, and greedy. They are not always reliable and may falter in following defined guidelines and best practices. Security professionals must install adequate prevention and detection controls and properly train all systems users Proper hiring and firing practices can eliminate certain risks. Security Awareness training is key to ensuring people are aware of risks and their responsibilities.

The following answers are incorrect:Software. Although software exploits are major threat and cause for concern, people are the weakest point in a security posture. Software can be removed, upgraded or patched to reduce risk.

Communications. Although many attacks from inside and outside an organization use communication methods such as the network infrastructure, this is not the weakest point in a security posture. Communications can be monitored, devices installed or upgraded to reduce risk and react to attack attempts.

Hardware. Hardware components can be a weakness in a security posture, but they are not the weakest link of the choices provided. Access to hardware can be minimized by such measures as installing locks and monitoring access in and out of certain areas.

The following reference(s) were/was used to create this question:

Shon Harris AIO v.3 P.19, 107-109
ISC2 OIG 2007, p.51-55

QUESTION 91
Which of the following is based on the premise that the quality of a software product is a direct function of the quality of its associated software development and maintenance processes?

A. The Software Capability Maturity Model (CMM)
B. The Spiral Model
C. The Waterfall Model
D. Expert Systems Model

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Capability Maturity Model (CMM) is a service mark owned by Carnegie Mellon University (CMU) and refers to a development model elicited from actual data. The data was collected from organizations that contracted with the U.S. Department of Defense, who funded the research, and became the foundation from which CMU created the Software Engineering Institute (SEI). Like any model, it is an abstraction of an existing system.

The Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process. The model describes a fivelevel evolutionary path of increasingly organized and systematically more mature processes. CMM was developed and is promoted by the Software Engineering Institute (SEI), a research and development center sponsored by the U.S. Department of Defense (DoD). SEI was founded in 1984 to address software engineering issues and, in a broad sense, to advance software engineering methodologies. More specifically, SEI was established to optimize the process of developing, acquiring, and maintaining heavily software-reliant systems for the DoD. Because the processes involved are equally applicable to the software industry as a whole, SEI advocates industry-wide adoption of the CMM.

The CMM is similar to ISO 9001, one of the ISO 9000 series of standards specified by the International Organization for Standardization (ISO). The ISO 9000 standards specify an effective quality system for manufacturing and service industries; ISO 9001 deals specifically with software development and maintenance. The main difference between the two systems lies in their respective purposes: ISO 9001 specifies a minimal acceptable quality level for software processes, while the CMM establishes a framework for continuous process improvement and is more explicit than the ISO standard in defining the means to be employed to that end.

CMM's Five Maturity Levels of Software Processes

At the initial level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.

At the repeatable level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been made established, defined, and documented.

At the defined level, an organization has developed its own standard software process through greater attention to documentation, standardization, and integration.

At the managed level, an organization monitors and controls its own processes through data collection and analysis.

At the optimizing level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

When it is applied to an existing organization's software development processes, it allows an effective approach toward improving them. Eventually it became clear that the model could be applied to other processes. This gave rise to a more general concept that is applied to business processes and to developing people.

CMM is superseded by CMMI

The CMM model proved useful to many organizations, but its application in software development has sometimes been problematic. Applying multiple models that are not integrated within and across an organization could be costly in terms of training, appraisals, and improvement activities. The Capability Maturity Model Integration (CMMI) project was formed to sort out the problem of using multiple CMMs.

For software development processes, the CMM has been superseded by Capability Maturity Model Integration (CMMI), though the CMM continues to be a general theoretical process capability model used in the public domain. CMM is adapted to processes other than software development

The CMM was originally intended as a tool to evaluate the ability of government contractors to perform a contracted software project. Though it comes from the area of software development, it can be, has been, and continues to be widely applied as a general model of the maturity of processes (e.g., IT Service Management processes) in IS/IT (and other) organizations.

Source:

http://searchsoftwarequality.techtarget.com/sDefinition/0,,sid92_gci930057,00.html
and
http://en.wikipedia.org/wiki/Capability_Maturity_Model

QUESTION 92
Which of the following determines that the product developed meets the projects goals?

A. verification
B. validation
C. concurrence
D. accuracy

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Software Development Verification vs. Validation:

Verification determines if the product accurately represents and meets the design specifications given to the developers. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met and closely followed by the development team.

Validation determines if the product provides the necessary solution intended real-world problem. It validates whether or not the final product is what the user expected in the first place and whether or not it solve the problem it intended to solve. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

NOTE:
DIACAP has replace DITSCAP but the definition above are still valid and applicable for the purpose of the exam.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw-Hill. Kindle Edition.
and
http://iase.disa.mil/ditscap/DITSCAP.html

QUESTION 93
Which of the following is the act of performing tests and evaluations to test a system's security level to see if it complies with the design specifications and security requirements?

A. Validation
B. Verification
C. Assessment
D. Accuracy

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Verification vs. Validation:

Verification determines if the product accurately represents and meets the specifications. A product can be developed that does not match the original specifications. This step ensures that the specifications are properly met.

Validation determines if the product provides the necessary solution intended real-world problem. In large projects, it is easy to lose sight of overall goal. This exercise ensures that the main goal of the project is met.

From DITSCAP:
6.3.2. Phase 2, Verification. The Verification phase shall include activities to verify compliance of the system with previously agreed security requirements. For each life-cycle development activity, DoD Directive 5000.1 (reference (i)), there is a corresponding set of security activities, enclosure 3, that shall verify compliance with the security requirements and evaluate vulnerabilities.

6.3.3. Phase 3, Validation. The Validation phase shall include activities to evaluate the fully integrated system to validate system operation in a specified computing environment with an acceptable level of residual risk. Validation shall culminate in an approval to operate.

You must also be familiar with Verification and Validation for the purpose of the exam. A simple definition for Verification would be whether or not the developers followed the design specifications along with the security requirements. A simple definition for Validation would be whether or not the final product meets the end user needs and can be use for a specific purpose.

Wikipedia has an informal description that is currently written as: Validation can be expressed by the query "Are you building the right thing?" and Verification by "Are you building it right?

NOTE:
DITSCAP was replaced by DIACAP some time ago (2007). While DITSCAP had defined both a verification and a validation phase, the DIACAP only has a validation phase. It may not make a difference in the answer for the exam; however, DIACAP is the cornerstone policy of DOD C&A and IA efforts today. Be familiar with both terms just in case all of a sudden the exam becomes updated with the new term.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1106). McGraw-Hill. Kindle Edition.

http://iase.disa.mil/ditscap/DITSCAP.html
https://en.wikipedia.org/wiki/Verification_and_validation
For the definition of "validation" in DIACAP, Click Here
Further sources for the phases in DIACAP, Click Here

QUESTION 94
Which of the following refers to the data left on the media after the media has been erased?

A. remanence
B. recovery
C. sticky bits
D. semi-hidden

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Actually the term "remanence" comes from electromagnetism, the study of the electromagnetics. Originally referred to (and still does in that field of study) the magnetic flux that remains in a magnetic circuit after an applied magnetomotive force has been removed. Absolutely no way a candidate will see anywhere near that much detail on any similar CISSP question, but having read this, a candidate won't be likely to forget it either.

It is becoming increasingly commonplace for people to buy used computer equipment, such as a hard drive, or router, and find information on the device left there by the previous owner; information they thought had been deleted. This is a classic example of data remanence: the remains of partial or even the entire data set of digital information. Normally, this refers to the data that remain on media after they are written over or degaussed. Data remanence is most common in storage systems but can also occur in memory.

Specialized hardware devices known as degaussers can be used to erase data saved to magnetic media. The measure of the amount of energy needed to reduce the magnetic field on the media to zero is known as coercivity.

It is important to make sure that the coercivity of the degausser is of sufficient strength to meet object reuse requirements when erasing data. If a degausser is used with insufficient coercivity, then a remanence of the data will exist. Remanence is the measure of the existing magnetic field on the media; it is the residue that remains after an object is degaussed or written over.

Data is still recoverable even when the remanence is small. While data remanence exists, there is no assurance of safe object reuse.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4207-4210). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19694-19699). Auerbach Publications. Kindle Edition.

QUESTION 95
Which of the following is NOT a basic component of security architecture?

A. Motherboard
B. Central Processing Unit (CPU
C. Storage Devices
D. Peripherals (input/output devices)

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The CPU, storage devices and peripherals each have specialized roles in the security archecture. The CPU, or microprocessor, is the brains behind a computer system and performs calculations as it solves problemes and performs system tasks. Storage devices provide both long- and short-term stoarge of information that the CPU has either processed or may process. Peripherals (scanners, printers, modems, etc) are devices that either input datra or receive the data output by the CPU.

The motherboard is the main circuit board of a microcomputer and contains the connectors for attaching additional boards. Typically, the motherboard contains the CPU, BIOS, memory, mass storage interfaces, serial and parallel ports, expansion slots, and all the controllers required to control standard peripheral devices.

Reference(s) used for this question:

TIPTON, Harold F., The Official (ISC)2 Guide to the CISSP CBK (2007), page 308.

QUESTION 96
Which of the following is a set of data processing elements that increases the performance in a computer by overlapping the steps of different instructions?

A. pipelining
B. complex-instruction-set-computer (CISC)
C. reduced-instruction-set-computer (RISC)
D. multitasking

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Pipelining is a natural concept in everyday life, e.g. on an assembly line. Consider the assembly of a car: assume that certain steps in the assembly line are to install the engine, install the hood, and install the wheels (in that order, with arbitrary interstitial steps). A car on the assembly line can have only one of the three steps done at once. After the car has its engine installed, it moves on to having its hood installed, leaving the engine installation facilities available for the next car. The first car then moves on to wheel installation, the second car to hood installation, and a third car begins to have its engine installed. If engine installation takes 20 minutes, hood installation takes 5 minutes, and wheel installation takes 10 minutes, then finishing all three cars when only one car can be assembled at once would take 105 minutes. On the other hand, using the assembly line, the total time to complete all three is 75 minutes. At this point, additional cars will come off the assembly line at 20 minute increments.

In computing, a pipeline is a set of data processing elements connected in series, so that the output of one element is the input of the next one. The elements of a pipeline are often executed in parallel or in time-sliced fashion; in that case, some amount of buffer storage is often inserted between elements. Pipelining is used in processors to allow overlapping execution of multiple instructions within the same circuitry. The circuitry is usually divided into stages, including instruction decoding, arithmetic, and register fetching stages, wherein each stage processes one instruction at a time.

The following were not correct answers:

CISC: is a CPU design where single instructions execute several low-level operations (such as a load from memory, an arithmetic operation, and a memory store) within a single instruction.

RISC: is a CPU design based on simplified instructions that can provide higher performance as the simplicity enables much faster execution of each instruction.

Multitasking: is a method where multiple tasks share common processing resources, such as a CPU, through a method of fast scheduling that gives the appearance of parallelism, but in reality only one task is being performed at any one time.

Reference:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, pages 188-189.
Also see
http://en.wikipedia.org/wiki/Pipeline_(computing)

QUESTION 97
Which of the following describes a computer processing architecture in which a language compiler or pre-processor breaks program instructions down into basic operations that can be performed by the processor at the same time?

A. Very-Long Instruction-Word Processor (VLIW)
B. Complex-Instruction-Set-Computer (CISC)
C. Reduced-Instruction-Set-Computer (RISC)
D. Super Scalar Processor Architecture (SCPA)

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Very long instruction word (VLIW) describes a computer processing architecture in which a language compiler or pre-processor breaks program instruction down into basic operations that can be performed by the processor in parallel (that is, at the same time). These operations are put into a very long instruction word which the processor can then take apart without further analysis, handing each operation to an appropriate functional unit.

The following answer are incorrect:

The term "CISC" (complex instruction set computer or computing) refers to computers designed with a full set of computer instructions that were intended to provide needed capabilities in the most efficient way. Later, it was discovered that, by reducing the full set to only the most frequently used instructions, the computer would get more work done in a shorter amount of time for most applications. Intel's Pentium microprocessors are CISC microprocessors.

The PowerPC microprocessor, used in IBM's RISC System/6000 workstation and Macintosh computers, is a RISC microprocessor. RISC takes each of the longer, more complex instructions from a CISC design and reduces it to multiple instructions that are shorter and faster to process. RISC technology has been a staple of mobile devices for decades, but it is now finally poised to take on a serious role in data center servers and server virtualization. The latest RISC processors support virtualization and will change the way computing resources scale to meet workload demands.

A superscalar CPU architecture implements a form of parallelism called instruction level parallelism within a single processor. It therefore allows faster CPU throughput than would otherwise be possible at a given clock rate. A superscalar processor executes more than one instruction during a clock cycle by simultaneously dispatching multiple instructions to redundant functional units on the processor. Each functional unit is not a separate CPU core but an execution resource within a single CPU such as an arithmetic logic unit, a bit shifter, or a multiplier.

Reference(s) Used for this question:
http://whatis.techtarget.com/definition/0,,sid9_gci214395,00.html
and
http://searchcio-midmarket.techtarget.com/definition/CISC
and
http://en.wikipedia.org/wiki/Superscalar

QUESTION 98
Which of the following addresses a portion of the primary memory by specifying the actual address of the memory location?

A. direct addressing
B. Indirect addressing
C. implied addressing
D. indexed addressing

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Absolute/Direct

```
+------+-----+--------------------------------------+
| load | reg |        address                       |
+------+-----+--------------------------------------+
```

(Effective address = address as given in instruction)

This requires space in an instruction for quite a large address. It is often available on CISC machines which have variable-length instructions, such as x86.

Some RISC machines have a special Load Upper Literal instruction which places a 16-bit constant in the top half of a register. An OR literal instruction can be used to insert a 16-bit constant in the lower half of that register, so that a full 32-bit address can then be used via the register-indirect addressing mode, which itself is provided as "base-plus-offset" with an offset of 0. http://en.wikipedia.org/wiki/Addressing_mode (Very good coverage of the subject)

also see:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, page 186. also see: http://www.comsci.us/ic/notes/am.html

QUESTION 99

Which of the following is NOT true concerning Application Control?

A. It limits end users use of applications in such a way that only particular screens are visible.
B. Only specific records can be requested through the application controls
C. Particular usage of the application can be recorded for audit purposes
D. It is non-transparent to the endpoint applications so changes are needed to the applications and databases involved

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, Auerbach.

QUESTION 100
Which of the following are NOT a countermeasure to traffic analysis?

A. Padding messages.
B. Eavesdropping.
C. Sending noise.
D. Faraday Cage

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Eavesdropping is not a countermeasure, it is a type of attack where you are collecting traffic and attempting to see what is being send between entities communicating with each other.

The following answers are incorrect:

Padding Messages. Is incorrect because it is considered a countermeasure you make messages uniform size, padding can be used to counter this kind of attack, in which decoy traffic is sent out over the network to disguise patterns and make it more difficult to uncover patterns.
Sending Noise. Is incorrect because it is considered a countermeasure, tansmitting non-informational data elements to disguise real data.

Faraday Cage Is incorrect because it is a tool used to prevent emanation of electromagnetic waves. It is a very effective tool to prevent traffic analysis.

QUESTION 101
Preservation of confidentiality within information systems requires that the information is not disclosed to:

A. Authorized person
B. Unauthorized persons or processes.
C. Unauthorized persons.
D. Authorized persons and processes

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Confidentiality assures that the information is not disclosed to unauthorized persons or processes.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 102
Which of the following is not one of the three goals of Integrity addressed by the Clark-Wilson model?

A. Prevention of the modification of information by unauthorized users.
B. Prevention of the unauthorized or unintentional modification of information by authorized users.
C. Preservation of the internal and external consistency.
D. Prevention of the modification of information by authorized users.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
There is no need to prevent modification from authorized users. They are authorized and allowed to make the changes. On top of this, it is also NOT one of the goal of Integrity within Clark-Wilson.

As it turns out, the Biba model addresses only the first of the three integrity goals which is Prevention of the modification of information by unauthorized users. Clark-Wilson addresses all three goals of integrity.

The Clark–Wilson model improves on Biba by focusing on integrity at the transaction level and addressing three major goals of integrity in a commercial environment. In addition to preventing changes by unauthorized subjects, Clark and Wilson realized that high-integrity systems would also have to prevent

undesirable changes by authorized subjects and to ensure that the system continued to behave consistently. It also recognized that it would need to ensure that there is constant mediation between every subject and every object if such integrity was going to be maintained.

Integrity is addressed through the following three goals:

1. Prevention of the modification of information by unauthorized users.
2. Prevention of the unauthorized or unintentional modification of information by authorized users.
3. Preservation of the internal and external consistency.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17689-17694). Auerbach Publications. Kindle Edition. and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 31.

QUESTION 103
External consistency ensures that the data stored in the database is:

A. in-consistent with the real world.

B. remains consistant when sent from one system to another.
C. consistent with the logical world.
D. consistent with the real world.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
External consistency ensures that the data stored in the database is consistent with the real world.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, page 33.

QUESTION 104
Which of the following would be best suited to oversee the development of an information security policy?

A. System Administrators
B. End User
C. Security Officers
D. Security administrators

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The security officer would be the best person to oversea the development of such policies.

Security officers and their teams have typically been charged with the responsibility of creating the security policies. The policies must be written and communicated appropriately to ensure that they can be understood by the end users. Policies that are poorly written, or written at too high of an education level (common industry practice is to focus the content for general users at the sixth- to eighth-grade reading level), will not be understood.

Implementing security policies and the items that support them shows due care by the company and its management staff. Informing employees of what is

expected of them and the consequences of noncompliance can come down to a liability issue.

While security officers may be responsible for the development of the security policies, the effort should be collaborative to ensure that the business issues are addressed.

The security officers will get better corporate support by including other areas in policy development. This helps build buy-in by these areas as they take on a greater ownership of the final product. Consider including areas such as HR, legal, compliance, various IT areas and specific business area representatives who represent critical business units.

When policies are developed solely within the IT department and then distributed without business input, they are likely to miss important business considerations. Once policy documents have been created, the basis for ensuring compliance is established. Depending on the organization, additional documentation may be necessary to support policy. This support may come in the form of additional controls described in standards, baselines, or procedures to help personnel with compliance. An important step after documentation is to make the most current version of the documents readily accessible to those who are expected to follow them. Many organizations place the documents on their intranets or in shared file folders to facilitate their accessibility. Such placement of these documents plus checklists, forms, and sample documents can make awareness more effective.

For your exam you should know the information below:

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Executive Management/Senior Management - Executive management maintains the overall responsibility for protection of the information assets. The business operations are dependent upon information being available, accurate, and protected from individuals without a need to know.

Security Officer - The security officer directs, coordinates, plans, and organizes information security activities throughout the organization. The security officer works with many different individuals, such as executive management, management of the business units, technical staff, business partners, auditors, and third parties such as vendors. The security officer and his or her team are responsible for the design, implementation, management, and review of the organization's security policies, standards, procedures, baselines, and guidelines.

Information Systems Security Professional- Drafting of security policies, standards and supporting guidelines, procedures, and baselines is coordinated through these individuals. Guidance is provided for technical security issues, and emerging threats are considered for the adoption of new policies. Activities such as interpretation of government regulations and industry trends and analysis of vendor solutions to include in the security architecture that advances the security of the organization are performed in this role.

Data/Information/Business/System Owners - A business executive or manager is typically responsible for an information asset. These are the individuals that assign the appropriate classification to information assets. They ensure that the business information is protected with appropriate controls. Periodically, the information asset owners need to review the classification and access rights associated with information assets. The owners, or their delegates, may be required to approve access to the information. Owners also need to determine the criticality, sensitivity, retention, backups, and safeguards for the information. Owners or their delegates are responsible for understanding the risks that exist with regards to the information that they control.

Data/Information Custodian/Steward - A data custodian is an individual or function that takes care of the information on behalf of the owner. These individuals ensure that the information is available to the end users and is backed up to enable recovery in the event of data loss or corruption. Information may be stored in files, databases, or systems whose technical infrastructure must be managed, by systems administrators. This group administers access rights to the information assets.

Information Systems Auditor- IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent

assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Business Continuity Planner - Business continuity planners develop contingency plans to prepare for any occurrence that could have the ability to impact the company's objectives negatively. Threats may include earthquakes, tornadoes, hurricanes, blackouts, changes in the economic/political climate, terrorist activities, fire, or other major actions potentially causing significant harm. The business continuity planner ensures that business processes can continue through the disaster and coordinates those activities with the business areas and information technology personnel responsible for disaster recovery.

Information Systems/ Technology Professionals- These personnel are responsible for designing security controls into information systems, testing the controls, and implementing the systems in production environments through agreed upon operating policies and procedures. The information systems professionals work with the business owners and the security professionals to ensure that the designed solution provides security controls commensurate with the acceptable criticality, sensitivity, and availability requirements of the application.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Network/Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

Physical Security - The individuals assigned to the physical security role establish relationships with external law enforcement, such as the local police agencies, state police, or the Federal Bureau of Investigation (FBI) to assist in investigations. Physical security personnel manage the installation, maintenance, and ongoing operation of the closed circuit television (CCTV) surveillance systems, burglar alarm systems, and card reader access control systems. Guards are placed where necessary as a deterrent to unauthorized access and to provide safety for the company employees. Physical security personnel interface with systems security, human resources, facilities, and legal and business areas to ensure that the practices are integrated.

Security Analyst - The security analyst role works at a higher, more strategic level than the previously described roles and helps develop policies, standards, and guidelines, as well as set various baselines. Whereas the previous roles are "in the weeds" and focus on pieces and parts of the security program, a security analyst helps define the security program elements and follows through to ensure the elements are being carried out and practiced properly. This person works more at a design level than at an implementation level.

Administrative Assistants/Secretaries - This role can be very important to information security; in many companies of smaller size, this may be the individual who greets visitors, signs packages in and out, recognizes individuals who desire to enter the offices, and serves as the phone screener for executives. These individuals may be subject to social engineering attacks, whereby the potential intruder attempts to solicit confidential information that may be used for a subsequent attack. Social engineers prey on the goodwill of the helpful individual to gain entry. A properly trained assistant will minimize the risk of divulging useful company information or of providing unauthorized entry.

Help Desk Administrator - As the name implies, the help desk is there to field questions from users that report system problems. Problems may include poor response time, potential virus infections, unauthorized access, inability to access system resources, or questions on the use of a program. The help desk is also often where the first indications of security issues and incidents will be seen. A help desk individual would contact the computer security incident response team (CIRT) when a situation meets the criteria developed by the team. The help desk resets passwords, resynchronizes/reinitializes tokens and smart cards, and resolves other problems with access control.

Supervisor - The supervisor role, also called user manager, is ultimately responsible for all user activity and any assets created and owned by these users. For example, suppose Kathy is the supervisor of ten employees. Her responsibilities would include ensuring that these employees understand their responsibilities with respect to security; making sure the employees' account information is up-to-date; and informing the security administrator when an employee is fired, suspended, or transferred. Any change that pertains to an employee's role within the company usually affects what access rights they should and should not have, so the user manager must inform the security administrator of these changes immediately.

Change Control Analyst Since the only thing that is constant is change, someone must make sure changes happen securely. The change control analyst is responsible for approving or rejecting requests to make changes to the network, systems, or software. This role must make certain that the change will not introduce any vulnerabilities, that it has been properly tested, and that it is properly rolled out. The change control analyst needs to understand how various changes can affect security, interoperability, performance, and productivity. Or, a company can choose to just roll out the change and see what happens.

The following answers are incorrect:

Systems Administrator - A systems administrator (sysadmin/netadmin) configures network and server hardware and the operating systems to ensure that the information can be available and accessible. The administrator maintains the computing infrastructure using tools and utilities such as patch management and software distribution mechanisms to install updates and test patches on organization computers. The administrator tests and implements system upgrades to ensure the continued reliability of the servers and network devices. The administrator provides vulnerability management through either commercial off the shelf (COTS) and/or non-COTS solutions to test the computing environment and mitigate vulnerabilities appropriately.

End User - The end user is responsible for protecting information assets on a daily basis through adherence to the security policies that have been communicated.

Security Administrator - A security administrator manages the user access request process and ensures that privileges are provided to those individuals who have been authorized for access by application/system/data owners. This individual has elevated privileges and creates and deletes accounts and access permissions. The security administrator also terminates access privileges when individuals leave their jobs or transfer between company divisions. The security

administrator maintains records of access request approvals and produces reports of access rights for the auditor during testing in an access controls audit to demonstrate compliance with the policies.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 109
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 108). McGraw-Hill. Kindle Edition.

QUESTION 105
Which of the following is the MOST important aspect relating to employee termination?

A. The details of employee have been removed from active payroll files.
B. Company property provided to the employee has been returned.
C. User ID and passwords of the employee have been deleted.
D. The appropriate company staff are notified about the termination.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Even though Logical access to information by a terminated employee is possible if the ID and password of the terminated employee has not been deleted this is only one part of the termination procedures. If user ID is not disabled or deleted, it could be possible for the employee without physical access to visit the companies networks remotely and gain access to the information.

Please note that this can also be seen in a different way: the most important thing to do could also be to inform others of the person's termination, because even if user ID's and passwords are deleted, a terminated individual could simply socially engineer their way back in by calling an individual he/she used to work with and ask them for access. He could intrude on the facility or use other weaknesses to gain access to information after he has been terminated.

By notifying the appropriate company staff about the termination, they would in turn intitiate account termination, ask the employee to return company property, and all credentials would be withdrawn for the individual concerned. This answer is more complete than simply disabling account.

It seems harsh and cold when this actually takes place , but too many companies have been hurt by vengeful employees who have lashed out at the company when their positions were revoked for one reason or another. If an employee is disgruntled in any way, or the termination is unfriendly, that employee’s accounts should be disabled right away, and all passwords on all systems changed.

For your exam you should know the information below:

Employee Termination Processes

Employees join and leave organizations every day. The reasons vary widely, due to retirement,reduction in force, layoffs, termination with or without cause, relocation to another city, careeropportunities with other employers, or involuntary transfers. Terminations may be friendly or unfriendly and will need different levels of care as a result.

Friendly Terminations
Regular termination is when there is little or no evidence or reason to believe that the termination is not agreeable to both the company and the employee. A standard set of procedures, typically maintained by the human resources department, governs the dismissal of the terminated employee to ensure that company property is returned, and all access is removed. These procedures may include exit interviews and return of keys, identification cards, badges, tokens, and cryptographic keys. Other property, such as laptops, cable locks, credit cards, and phone cards, are also collected. The user manager notifies the security department of the termination to ensure that access is revoked for all platforms and facilities. Some facilities choose to immediately delete the accounts, while others choose to disable the accounts for a policy defined period, for example, 30 days, to account for changes or extensions in the final termination date. The termination process should include a conversation with the departing associate about their continued responsibility for confidentiality of information.

Unfriendly Terminations
Unfriendly terminations may occur when the individual is fired, involuntarily transferred, laid off,or when the organization has reason to believe that the individual has the means and intention to potentially cause harm to the system. Individuals with technical skills and higher levels of access, such as the systems administrators, computer programmers, database administrators, or any individual with elevated privileges, may present higher risk to the environment. These individuals could alter files, plant logic bombs to create system file damage at a future date, or remove sensitive information. Other disgruntled users could enter erroneous data into the system that may not be discovered for several months. In these situations, immediate termination of systems access is warranted at the time of termination or prior to notifying the employee of the termination. Managing the people aspect of security, from pre-employment to postemployment, is critical to ensure that trustworthy, competent resources are employed to further the business objectives that will protect company information. Each of these actions contributes to preventive, detective, or corrective personnel controls.

The following answers are incorrect:
The other options are less important.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 99
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 129). McGraw-Hill. Kindle Edition.

QUESTION 106
Making sure that only those who are supposed to access the data can access is which of the following?

A. confidentiality.
B. capability.
C. integrity.
D. availability.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate, domain definition. Confidentiality is making sure that only those who are supposed to access the data can access it.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 107
Related to information security, confidentiality is the opposite of which of the following?

A. closure
B. disclosure
C. disposal
D. disaster

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Confidentiality is the opposite of disclosure.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 108
Related to information security, integrity is the opposite of which of the following?

A. abstraction
B. alteration
C. accreditation
D. application

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

Integrity is the opposite of "alteration."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 109
Making sure that the data is accessible when and where it is needed is which of the following?

A. confidentiality
B. integrity
C. acceptability
D. availability

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Availability is making sure that the data is accessible when and where it is needed.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 110
Related to information security, availability is the opposite of which of the following?

A. delegation
B. distribution
C. documentation
D. destruction

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Availability is the opposite of "destruction."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 59.

QUESTION 111
Related to information security, the prevention of the intentional or unintentional unauthorized disclosure of contents is which of the following?

A. Confidentiality
B. Integrity
C. Availability
D. capability

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Confidentiality is the prevention of the intentional or unintentional unauthorized disclosure of contents.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

QUESTION 112
Related to information security, the guarantee that the message sent is the message received with the assurance that the message was not intentionally or unintentionally altered is an example of which of the following?

A. integrity
B. confidentiality
C. availability
D. identity

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 60.

QUESTION 113
One of the following assertions is NOT a characteristic of Internet Protocol Security (IPsec)

A. Data cannot be read by unauthorized parties
B. The identity of all IPsec endpoints are confirmed by other endpoints
C. Data is delivered in the exact order in which it is sent
D. The number of packets being exchanged can be counted.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
IPSec provide replay protection that ensures data is not delivered multiple times, however IPsec does not ensure that data is delivered in the exact order in which it is sent. IPSEC uses TCP and packets may be delivered out of order to the receiving side depending which route was taken by the packet.

Internet Protocol Security (IPsec) has emerged as the most commonly used network layer security control for protecting communications. IPsec is a framework of open standards for ensuring private communications over IP networks. Depending on how IPsec is implemented and configured, it can provide any combination of the following types of protection:

Confidentiality. IPsec can ensure that data cannot be read by unauthorized parties. This is accomplished by encrypting data using a cryptographic algorithm and a secret key a value known only to the two parties exchanging data. The data can only be decrypted by someone who has the secret key.

Integrity. IPsec can determine if data has been changed (intentionally or unintentionally) during transit. The integrity of data can be assured by generating a message authentication code (MAC) value, which is a cryptographic checksum of the data. If the data is altered and the MAC is recalculated, the old and new MACs will differ.

Peer Authentication. Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

Replay Protection. The same data is not delivered multiple times, and data is not delivered grossly out of order. However, IPsec does not ensure that data is delivered in the exact order in which it is sent.

Traffic Analysis Protection. A person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged. However, the number of packets being exchanged can be counted.

Access Control. IPsec endpoints can perform filtering to ensure that only authorized IPsec users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing Web server access but denying file sharing.

The following are incorrect answers because they are all features provided by IPSEC:

"Data cannot be read by unauthorized parties" is wrong because IPsec provides confidentiality through the usage of the Encapsulating Security Protocol (ESP), once encrypted the data cannot be read by unauthorized parties because they have access only to the ciphertext. This is accomplished by encrypting data using a cryptographic algorithm and a session key, a value known only to the two parties exchanging data. The data can only be decrypted by someone who has a copy of the session key.

"The identity of all IPsec endpoints are confirmed by other endpoints" is wrong because IPsec provides peer authentication: Each IPsec endpoint confirms the identity of the other IPsec endpoint with which it wishes to communicate, ensuring that the network traffic and data is being sent from the expected host.

"The number of packets being exchanged can be counted" is wrong because although IPsec provides traffic protection where a person monitoring network traffic does not know which parties are communicating, how often communications are occurring, or how much data is being exchanged, the number of packets being exchanged still can be counted.

Reference(s) used for this question:
NIST 800-77 Guide to IPsec VPNs . Pages 2-3 to 2-4

QUESTION 114
One of these statements about the key elements of a good configuration process is NOT true

A. Accommodate the reuse of proven standards and best practices
B. Ensure that all requirements remain clear, concise, and valid
C. Control modifications to system hardware in order to prevent resource changes
D. Ensure changes, standards, and requirements are communicated promptly and precisely

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Configuration management isn't about preventing change but ensuring the integrity of IT resources by preventing unauthorised or improper changes.

According to the Official ISC2 guide to the CISSP exam, a good CM process is one that can:

(1) accommodate change;
(2) accommodate the reuse of proven standards and best practices;
(3) ensure that all requirements remain clear, concise, and valid;
(4) ensure changes, standards, and requirements are communicated promptly and precisely; and
(5) ensure that the results conform to each instance of the product.

Configuration management
Configuration management (CM) is the detailed recording and updating of information that describes an enterprise's computer systems and networks, including all hardware and software components. Such information typically includes the versions and updates that have been applied to installed software packages and the locations and network addresses of hardware devices. Special configuration management software is available. When a system needs a hardware or software upgrade, a computer technician can accesses the configuration management program and database to see what is currently installed. The technician can then make a more informed decision about the upgrade needed.

An advantage of a configuration management application is that the entire collection of systems can be reviewed to make sure any changes made to one system do not adversely affect any of the other systems

Configuration management is also used in software development, where it is called Unified Configuration Management (UCM). Using UCM, developers can keep track of the source code, documentation, problems, changes requested, and changes made. Change management
In a computer system environment, change management refers to a systematic approach to keeping track of the details of the system (for example, what operating system release is running on each computer and which fixes have been applied).

QUESTION 115
An area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability can be defined as:

A. Netware availability
B. Network availability
C. Network acceptability
D. Network accountability

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Network availability can be defined as an area of the Telecommunications and Network Security domain that directly affects the Information Systems Security tenet of Availability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 116
Risk analysis is MOST useful when applied during which phase of the system development process?

A. Project initiation and Planning
B. Functional Requirements definition
C. System Design Specification
D. Development and Implementation

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

In most projects the conditions for failure are established at the beginning of the project. Thus risk management should be established at the commencement of the project with a risk assessment during project initiation.

As it is clearly stated in the ISC2 book: Security should be included at the first phase of development and throughout all of the phases of the system development life cycle. This is a key concept to understand for the purpose for the exam.

The most useful time is to undertake it at project initiation, although it is often valuable to update the current risk analysis at later stages.

Attempting to retrofit security after the SDLC is completed would cost a lot more money and might be impossible in some cases. Look at the family of browsers we use today, for the past 8 years they always claim that it is the most secure version that has been released and within days vulnerabilities will be found.

Risks should be monitored throughout the SDLC of the project and reassessed when appropriate.

The phases of the SDLC can very from one source to another one. It could be as simple as Concept, Design, and Implementation. It could also be expanded to include more phases such as this list proposed within the ISC2 Official Study book:

Project Initiation and Planning
Functional Requirements Definition
System Design Specification

Development and Implementation
Documentations and Common Program Controls
Testing and Evaluation Control, certification and accreditation (C&A)
Transition to production (Implementation)

And there are two phases that will extend beyond the SDLC, they are:

Operation and Maintenance Support (O&M)
Revisions and System Replacement (Disposal)

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 291). and
The Official ISC2 Guide to the CISSP CBK , Second Edition, Page 182-185

QUESTION 117
Which of the following would MOST likely ensure that a system development project meets business objectives?

A. Development and tests are run by different individuals
B. User involvement in system specification and acceptance
C. Development of a project plan identifying all development activities

D. Strict deadlines and budgets

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Effective user involvement is the most critical factor in ensuring that the application meets business objectives.

A great way of getting early input from the user community is by using Prototyping. The prototyping method was formally introduced in the early 1980s to combat the perceived weaknesses of the waterfall model with regard to the speed of development. The objective is to build a simplified version (prototype) of the application, release it for review, and use the feedback from the users' review to build a second, better version.

This is repeated until the users are satisfied with the product. t is a four-step process:

initial concept,
design and implement initial prototype,
refine prototype until acceptable, and
complete and release final version.

There is also the Modified Prototype Model (MPM. This is a form of prototyping that is ideal for Web application development. It allows for the basic functionality of a desired system or component to be formally deployed in a quick time frame. The maintenance phase is set to begin after the deployment. The goal is to have the process be flexible enough so the application is not based on the state of the organization at any given time. As the organization grows and the environment changes, the application evolves with it, rather than being frozen in time.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12101-12108 and 12099-12101). Auerbach Publications. Kindle Edition.
and
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

QUESTION 118
What is RAD?

A. A development methodology
B. A project management technique
C. A measure of system complexity

D. Risk-assessment diagramming

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
RAD stands for Rapid Application Development.

RAD is a methodology that enables organizations to develop strategically important systems faster while reducing development costs and maintaining quality.

RAD is a programming system that enables programmers to quickly build working programs.

In general, RAD systems provide a number of tools to help build graphical user interfaces that would normally take a large development effort.

Two of the most popular RAD systems for Windows are Visual Basic and Delphi. Historically, RAD systems have tended to emphasize reducing development time, sometimes at the expense of generating in-efficient executable code. Nowadays, though, many RAD systems produce extremely faster code that is optimized.

Conversely, many traditional programming environments now come with a number of visual tools to aid development. Therefore, the line between RAD systems and other development environments has become blurred.

Reference:

Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 307)
http://www.webopedia.com

QUESTION 119
Which of the following best describes the purpose of debugging programs?

A. To generate random data that can be used to test programs before implementing them.
B. To ensure that program coding flaws are detected and corrected.
C. To protect, during the programming phase, valid changes from being overwritten by other changes.
D. To compare source code versions before transferring to the test environment

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Debugging provides the basis for the programmer to correct the logic errors in a program under development before it goes into production.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 298).

QUESTION 120
Which of the following would best describe the difference between white-box testing and black-box testing?

A. White-box testing is performed by an independent programmer team.
B. Black-box testing uses the bottom-up approach.
C. White-box testing examines the program internal logical structure.
D. Black-box testing involves the business units

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Black-box testing observes the system external behavior, while white-box testing is a detailed exam of a logical path, checking the possible conditions.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 121
Which of the following is a not a preventative control?

A. Deny programmer access to production data.
B. Require change requests to include information about dates, descriptions, cost analysis and anticipated effects.
C. Run a source comparison program between control and current source periodically.
D. Establish procedures for emergency changes.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Running the source comparison program between control and current source periodically allows detection, not prevention, of unauthorized changes in the production environment. Other options are preventive controls.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 122
Which of the following would provide the BEST stress testing environment taking under consideration and avoiding possible data exposure and leaks of sensitive data?

A. Test environment using test data.
B. Test environment using sanitized live workloads data.
C. Production environment using test data.
D. Production environment using sanitized live workloads data.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The best way to properly verify an application or system during a stress test would be to expose it to "live" data that has been sanitized to avoid exposing any sensitive information or Personally Identifiable Data (PII) while in a testing environment. Fabricated test data may not be as varied, complex or computationally demanding as "live" data. A production environment should never be used to test a product, as a production environment is one where the application or system is being put to commercial or operational use. It is a best practice to perform testing in a non-production environment.

Stress testing is carried out to ensure a system can cope with production workloads, but as it may be tested to destruction, a test environment should always be used to avoid damaging the production environment. Hence, testing should never take place in a production environment. If only test data is used, there is no certainty that the system was adequately stress tested.
Incorrect answers:

Test environment using test data. This is incorrect because live data is typically more useful during stress testing

Production environment using test data. This is incorrect because the production environment should not be used for testing.

Production environment using live workloads. This is incorrect because the production environment should not be used for testing.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299). And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 251.
And:

QUESTION 123

Which of the following BEST explains why computerized information systems frequently fail to meet the needs of users?

A. Inadequate quality assurance (QA) tools.
B. Constantly changing user needs.
C. Inadequate user participation in defining the system's requirements.
D. Inadequate project management.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Inadequate user participation in defining the system's requirements. Most projects fail to meet the needs of the users because there was inadequate input in the initial steps of the project from the user community and what their needs really are.

The other answers, while potentially valid, are incorrect because they do not represent the most common problem assosciated with information systems failing to meet the needs of users.

References: All in One pg 834

Only users can define what their needs are and, therefore, what the system should accomplish. Lack of adequate user involvement, especially in the systems requirements phase, will usually result in a system that doesn't fully or adequately address the needs of the user.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 296).

QUESTION 124
Which of the following would be the MOST serious risk where a systems development life cycle methodology is inadequate?

A. The project will be completed late.
B. The project will exceed the cost estimates.
C. The project will be incompatible with existing systems.
D. The project will fail to meet business and user needs.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

This is the most serious risk of inadequate systems development life cycle methodolgy.

The following answers are incorrect because :

The project will be completed late is incorrect as it is not most devastating as the above answer.

The project will exceed the cost estimates is also incorrect when compared to the above correct answer.

The project will be incompatible with existing systems is also incorrect when compared to the above correct answer.

Reference: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 290).

QUESTION 125
Which of the following is an advantage of prototyping?

A. Prototype systems can provide significant time and cost savings.
B. Change control is often less complicated with prototype systems.
C. It ensures that functions or extras are not added to the intended system.
D. Strong internal controls are easier to implement.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Prototype systems can provide significant time and cost savings, however they also have several disadvantages. They often have poor internal controls, change control becomes much more complicated and it often leads to functions or extras being added to the system that were not originally intended.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 306).

QUESTION 126
Which of the following is a CHARACTERISTIC of a decision support system (DSS) in regards to Threats and Risks Analysis?

A. DSS is aimed at solving highly structured problems.
B. DSS emphasizes flexibility in the decision making approach of users.
C. DSS supports only structured decision-making tasks.
D. DSS combines the use of models with non-traditional data access and retrieval functions.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
DSS emphasizes flexibility in the decision-making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semi-structured decision-making tasks.

DSS is sometimes referred to as the Delphi Method or Delphi Technique:
The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others' thought processes and enables them to participate in an independent and anonymous way. Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis. The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group. The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

Here is the ISC2 book coverage of the subject:
One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).

EXAM TIP:
The DSS is what some of the books are referring to as the Delphi Method or Delphi Technique. Be familiar with both terms for the purpose of the exam.

The other answers are incorrect:

'DSS is aimed at solving highly structured problems' is incorrect because it is aimed at solving less structured problems.

'DSS supports only structured decision-making tasks' is also incorrect as it supports semi-structured decision-making tasks.

'DSS combines the use of models with non-traditional data access and retrieval functions' is also incorrect as it combines the use of models and analytic techniques with traditional data access and retrieval functions.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 91). McGraw-Hill. Kindle Edition.
and

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 1424-1426). Auerbach Publications. Kindle Edition.

QUESTION 127
Which of the following is an advantage in using a bottom-up versus a top-down approach to software testing?

A. Interface errors are detected earlier.
B. Errors in critical modules are detected earlier.
C. Confidence in the system is achieved earlier.
D. Major functions and processing are tested earlier.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The bottom-up approach to software testing begins with the testing of atomic units, such as programs and modules, and work upwards until a complete system testing has taken place. The advantages of using a bottom-up approach to software testing are the fact that there is no need for stubs or drivers and errors in critical modules are found earlier. The other choices refer to advantages of a top down approach which follows the opposite path.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 299).

QUESTION 128
Which of the following would be the best reason for separating the test and development environments?

A. To restrict access to systems under test.
B. To control the stability of the test environment.
C. To segregate user and development staff.
D. To secure access to systems under development.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
The test environment must be controlled and stable in order to ensure that development projects are tested in a realistic environment which, as far as possible, mirrors the live environment.

Reference(s) used for this question:
Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 309).

QUESTION 129
What would BEST define a covert channel?

A. An undocumented backdoor that has been left by a programmer in an operating system
B. An open system port that should be closed.
C. A communication channel that allows transfer of information in a manner that violates the system's security policy.
D. A trojan horse.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Answer: A communication channel that allows transfer of information in a manner that violates the system's security policy.

A covert channel is a way for an entity to receive information in an unauthorized manner. It is an information flow that is not controlled by a security mechanism. This type of information path was not developed for communication; thus, the system does not properly protect this path, because the developers never envisioned information being passed in this way.

Receiving information in this manner clearly violates the system's security policy. The channel to transfer this unauthorized data is the result of one of the following conditions:• Oversight in the development of the product

• Improper implementation of access controls
• Existence of a shared resource between the two entities
• Installation of a Trojan horse

The following answers are incorrect:

An undocumented backdoor that has been left by a programmer in an operating system is incorrect because it is not a means by which unauthorized transfer of information takes place. Such backdoor is usually referred to as a Maintenance Hook.

An open system port that should be closed is incorrect as it does not define a covert channel.

A trojan horse is incorrect because it is a program that looks like a useful program but when you install it it would include a bonus such as a Worm, Backdoor, or some other malware without the installer knowing about it.

Reference(s) used for this question:

Shon Harris AIO v3 , Chapter-5 : Security Models & Architecture
AIOv4 Security Architecture and Design (pages 343 - 344)
AIOv5 Security Architecture and Design (pages 345 - 346)

QUESTION 130
Which of the following is NOT an administrative control?

A. Logical access control mechanisms
B. Screening of personnel
C. Development of policies, standards, procedures and guidelines
D. Change control procedures

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
It is considered to be a technical control.

Logical is synonymous with Technical Control. That was the easy answer.

There are three broad categories of access control: Administrative, Technical, and Physical.

Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.

Each category of access control has several components that fall within it, as shown here:

Administrative Controls

- Policy and procedures
- Personnel controls
- Supervisory structure
- Security-awareness training
- Testing

Physical Controls

Network segregation
Perimeter security
Computer controls
Work area separation
Data backups

Technical Controls

System access
Network architecture
Network access
Encryption and protocols
Control zone
Auditing

The following answers are incorrect :

Screening of personnel is considered to be an administrative control

Development of policies, standards, procedures and guidelines is considered to be an administrative control

Change control procedures is considered to be an administrative control.
Reference : Shon Harris AIO v3 , Chapter - 3 : Security Management Practices , Page : 52-54

QUESTION 131
Which of the following is NOT a technical control?

A. Password and resource management
B. Identification and authentication methods

C. Monitoring for physical intrusion
D. Intrusion Detection Systems

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
It is considered to be a 'Physical Control'

There are three broad categories of access control: administrative, technical, and physical. Each category has different access control mechanisms that can be carried out manually or automatically. All of these access control mechanisms should work in concert with each other to protect an infrastructure and its data.

Each category of access control has several components that fall within it, a partial list is shown here. Not all controls fall into a single category, many of the controls will be in two or more categories. Below you have an example with backups where it is in all three categories:

Administrative Controls
Policy and procedures

- A backup policy would be in place

Personnel controls
Supervisory structure
Security-awareness training
Testing
Physical Controls
Network segregation
Perimeter security
Computer controls
Work area separation

Data backups (actual storage of the media, i:e Offsite Storage Facility)

Cabling
Technical Controls
System access
Network architecture
Network access

Encryption and protocols
Control zone
Auditing
Backup (Actual software doing the backups)

The following answers are incorrect :

Password and resource management is considered to be a logical or technical control.

Identification and authentication methods is considered to be a logical or technical control.

Intrusion Detection Systems is considered to be a logical or technical control.
Reference : Shon Harris , AIO v3 , Chapter - 4 : Access Control , Page : 180 - 185

QUESTION 132
Which of the following is BEST defined as a physical control?

A. Monitoring of system activity
B. Fencing
C. Identification and authentication methods
D. Logical access control mechanisms

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Physical controls are items put into place to protect facility, personnel, and resources. Examples of physical controls are security guards, locks, fencing, and lighting.

The following answers are incorrect answers:

Monitoring of system activity is considered to be administrative control.

Identification and authentication methods are considered to be a technical control.

Logical access control mechanisms is also considered to be a technical control.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 1280-1282). McGraw-Hill. Kindle Edition.

QUESTION 133
Which of the following is given the responsibility of the maintenance and protection of the data?

A. Data owner
B. Data custodian
C. User
D. Security administrator

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
It is usually responsible for maintaining and protecting the data.

The following answers are incorrect:

Data owner is usually a member of management , in charge of a specific business unit and is ultimately responsible for the protection and use of the information.

User is any individual who routinely uses the data for work-related tasks.

Security administrator's tasks include creating new system user accounts , implementing new security software.
References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 99 - 103

QUESTION 134
Who should DECIDE how a company should approach security and what security measures should be implemented?

A. Senior management
B. Data owner
C. Auditor
D. The information security specialist

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
They are responsible for security of the organization and the protection of its assets.

The following answers are incorrect because :

Data owner is incorrect as data owners should not decide as to what security measures should be applied.

Auditor is also incorrect as auditor cannot decide as to what security measures should be applied.

The information security specialist is also incorrect as they may have the technical knowledge of how security measures should be implemented and configured , but they should not be in a position of deciding what measures should be applied.

Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 51.

QUESTION 135
Which of the following is responsible for MOST of the security issues?

A. Outside espionage
B. Hackers
C. Personnel
D. Equipment failure

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Personnel cause more security issues than hacker attacks, outside espionage, or equipment failure.

The following answers are incorrect because:

Outside espionage is incorrect as it is not the best answer.
Hackers is also incorrect as it is not the best answer.
Equipment failure is also incorrect as it is not the best answer.
Reference : Shon Harris AIO v3 , Chapter-3: Security Management Practices , Page : 56

QUESTION 136
What are the three FUNDAMENTAL principles of security?

A. Accountability, confidentiality and integrity
B. Confidentiality, integrity and availability
C. Integrity, availability and accountability

D. Availability, accountability and confidentiality

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The following answers are incorrect because:

Accountability, confidentiality and integrity is not the correct answer as Accountability is not one of the fundamental principle of security.

Integrity, availability and accountability is not the correct answer as Accountability is not one of the fundamental principle of security.

Availability, accountability and confidentiality is not the correct answer as Accountability is not one of the fundamental objective of security.

References : Shon Harris AIO v3 , Chapter - 3: Security Management Practices , Pages : 49-52

QUESTION 137
Within the context of the CBK, which of the following provides a MINIMUM level of security ACCEPTABLE for an environment ?

A. A baseline
B. A standard
C. A procedure
D. A guideline

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Baselines provide the minimum level of security necessary throughout the organization.

Standards specify how hardware and software products should be used throughout the organization.

Procedures are detailed step-by-step instruction on how to achieve certain tasks.

Guidelines are recommendation actions and operational guides to personnel when a specific standard does not apply.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 3: Security Management Practices (page 94).

QUESTION 138

According to private sector data classification levels, how would salary levels and medical information be classified?

A. Public.
B. Internal Use Only.
C. Restricted.
D. Confidential.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Typically there are three to four levels of information classification used by most organizations:
Confidential: Information that, if released or disclosed outside of the organization, would create severe problems for the organization. For example, information that provides a competitive advantage is important to the technical or financial success (like trade secrets, intellectual property, or research designs), or protects the privacy of individuals would be considered confidential. Information may include payroll information, health records, credit information, formulas, technical designs, restricted regulatory information, senior management internal correspondence, or business strategies or plans. These may also be called top secret, privileged, personal, sensitive, or highly confidential. In other words this information is ok within a defined group in the company such as marketing or sales, but is not suited for release to anyone else in the company without permission.

The following answers are incorrect:

Public: Information that may be disclosed to the general public without concern for harming the company, employees, or business partners. No special protections are required, and information in this category is sometimes referred to as unclassified. For example, information that is posted to a company's public Internet site, publicly released announcements, marketing materials, cafeteria menus, and any internal documents that would not present harm to the company if they were disclosed would be classified as public. While there is little concern for confidentiality, integrity and availability should be considered.

Internal Use Only: Information that could be disclosed within the company, but could harm the company if disclosed externally. Information such as customer lists, vendor pricing, organizational policies, standards and procedures, and internal organization announcements would need baseline security protections, but do not rise to the level of protection as confidential information. In other words, the information may be used freely within the company but any unapproved use outside the company can pose a chance of harm.

Restricted: Information that requires the utmost protection or, if discovered by unauthorized personnel, would cause irreparable harm to the organization would have the highest level of classification. There may be very few pieces of information like this within an organization, but data classified at this level requires all the access control and protection mechanisms available to the organization. Even when information classified at this level exists, there will be few copies of it

Reference(s) Used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 952-976). Auerbach Publications. Kindle Edition.

QUESTION 139
Which of the following would be the best criterion to consider in determining the classification of an information asset?

A. Value
B. Age
C. Useful life
D. Personal association

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Information classification should be based on the value of the information to the organization and its sensitivity (reflection of how much damage would accrue due to disclosure).

Age is incorrect. While age might be a consideration in some cases, the guiding principles should be value and sensitivity.

Useful life. While useful lifetime is relevant to how long data protections should be applied, the classification is based on information value and sensitivity.

Personal association is incorrect. Information classification decisions should be based on value of the information and its sensitiviry.

References
CBK, pp. 101 - 102.

QUESTION 140
Which of the following is not a responsibility of an information (data) owner?

A. Determine what level of classification the information requires.
B. Periodically review the classification assignments against business needs.
C. Delegate the responsibility of data protection to data custodians.
D. Running regular backups and periodically testing the validity of the backup data.

Correct Answer: D

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
This responsibility would be delegated to a data custodian rather than being performed directly by the information owner.

"Determine what level of classification the information requires" is incorrect. This is one of the major responsibilities of an information owner.

"Periodically review the classification assignments against business needs" is incorrect. This is one of the major responsibilities of an information owner.

"Delegates responsibility of maintenance of the data protection mechanisms to the data custodian" is incorrect. This is a responsibility of the information owner.

References:
CBK p. 105.
AIO3, p. 53-54, 960

QUESTION 141
Which of the following does not address Database Management Systems (DBMS) Security?

A. Perturbation
B. Cell suppression
C. Padded cells
D. Partitioning

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Padded cells complement Intrusion Detection Systems (IDSs) and are not related to DBMS security. Padded cells are simulated environments to which IDSs seamlessly transfer detected attackers and are designed to convince an attacker that the attack is going according to the plan. Cell suppression is a technique used against inference attacks by not revealing information in the case where a statistical query produces a very small result set. Perturbation also addresses inference attacks but involves making minor modifications to the results to a query. Partitioning involves splitting a database into two or more physical or logical parts; especially relevant for multilevel secure databases.

Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 142
Which of the following security modes of operation involves the highest risk?

A. Compartmented Security Mode
B. Multilevel Security Mode
C. System-High Security Mode
D. Dedicated Security Mode

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
In multilevel mode, two or more classification levels of data exist, some people are not cleared for all the data on the system.

Risk is higher because sensitive data could be made available to someone not validated as being capable of maintaining secrecy of that data (i.e., not cleared for it).

In other security modes, all users have the necessary clearance for all data on the system.
Source: LaROSA, Jeanette (domain leader), Application and System Development Security CISSP Open Study Guide, version 3.0, January 2002.

QUESTION 143
During which phase of an IT system life cycle are security requirements developed?

A. Operation
B. Initiation
C. Functional design analysis and Planning
D. Implementation

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The software development life cycle (SDLC) (sometimes referred to as the System Development Life Cycle) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems.

The NIST SP 800-64 revision 2 has within the description section of para 3.2.1:

This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

• Conduct the risk assessment and use the results to supplement the baseline security controls;

• Analyze security requirements;
• Perform functional and security testing;
• Prepare initial documents for system certification and accreditation; and
• Design security architecture.

Reviewing this publication you may want to pick development/acquisition. Although initiation would be a decent choice, it is correct to say during this phase you would only brainstorm the idea of security requirements. Once you start to develop and acquire hardware/software components then you would also develop the security controls for these. The Shon Harris reference below is correct as well.

Shon Harris' Book (All-in-One CISSP Certification Exam Guide) divides the SDLC differently:

Project initiation
Functional design analysis and planning
System design specifications
Software development
Installation
Maintenance support
Revision and replacement

According to the author (Shon Harris), security requirements should be developed during the functional design analysis and planning phase.
SDLC POSITIONING FROM NIST 800-64

FIGURE 2-1. POSITIONING SECURITY CONSIDERATIONS

SDLC Positioning in the enterprise

Information system security processes and activities provide valuable input into managing IT systems and their development, enabling risk identification, planning and mitigation. A risk management approach involves continually balancing the protection of agency information and assets with the cost of security controls and mitigation strategies throughout the complete information system development life cycle (see Figure 2-1 above). The most effective way to implement risk management is to identify critical assets and operations, as well as systemic vulnerabilities across the agency. Risks are shared and not bound by organization, revenue source, or topologies. Identification and verification of critical assets and operations and their interconnections can be achieved through the system security planning process, as well as through the compilation of information from the Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA) processes to establish insight into the agency's vital business operations, their supporting assets, and existing interdependencies and relationships.

With critical assets and operations identified, the organization can and should perform a business impact analysis (BIA). The purpose of the BIA is to relate systems and assets with the critical services they provide and assess the consequences of their disruption. By identifying these systems, an agency can manage security effectively by establishing priorities. This positions the security office to facilitate the IT program's cost-effective performance as well as articulate its business impact and value to the agency.

SDLC OVERVIEW FROM NIST 800-64
SDLC Overview from NIST 800-64 Revision 2

NIST 800-64 Revision 2 is one publication within the NISTstandards that I would recommend you look at for more details about the SDLC. It describe in great details what activities would take place and they have a nice diagram for each of the phases of the SDLC. You will find a copy at:

http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

DISCUSSION:
Different sources present slightly different info as far as the phases names are concerned.

People sometimes gets confused with some of the NIST standards. For example NIST 800-64 Security Considerations in the Information System Development Life Cycle has slightly different names, the activities mostly remains the same.

NIST clearly specifies that Security requirements would be considered throughout ALL of the phases. The keyword here is considered, if a question is about which phase they would be developed than Functional Design Analysis would be the correct choice.

Within the NIST standard they use different phase, howeverr under the second phase you will see that they talk specifically about Security Functional requirements analysis which confirms it is not at the initiation stage so it become easier to come out with the answer to this question. Here is what is stated:

The security functional requirements analysis considers the system security environment, including the enterprise information security policy and the enterprise security architecture. The analysis should address all requirements for confidentiality, integrity, and availability of information, and should include a review of all legal, functional, and other security requirements contained in applicable laws, regulations, and guidance.

At the initiation step you would NOT have enough detailed yet to produce the Security Requirements. You are mostly brainstorming on all of the issues listed but you do not develop them all at that stage.

By considering security early in the information system development life cycle (SDLC), you may be able to avoid higher costs later on and develop a more secure system from the start.

NIST says:
NIST`s Information Technology Laboratory recently issued Special Publication (SP) 800-64, Security Considerations in the Information System Development Life Cycle, by Tim Grance, Joan Hash, and Marc Stevens, to help organizations include security requirements in their planning for every phase of the system life cycle, and to select, acquire, and use appropriate and cost-effective security controls.

I must admit this is all very tricky but reading skills and paying attention to KEY WORDS is a must for this exam.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Page 956
and
NIST S-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
and http://www.mks.com/resources/resource-pages/software-development-life-cycle-sdlc-system-development

QUESTION 144
Which of the following phases of a system development life-cycle is most concerned with establishing a good security policy as the foundation for design?

A. Development/acquisition
B. Implementation

C. Initiation
D. Maintenance

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement.

The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support, and these goals guide the procedures, standards and controls used in the IT security architecture design.

The policy also should require definition of critical assets, the perceived threat, and security-related roles and responsibilities.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 6).

QUESTION 145
When considering an IT System Development Life-cycle, security should be:

A. Mostly considered during the initiation phase.
B. Mostly considered during the development phase.
C. Treated as an integral part of the overall system design.
D. Added once the design is completed.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes establishing security policies, understanding the resulting security requirements, participating in the evaluation of security products, and finally in the engineering, design, implementation, and disposal of the system.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 7).

QUESTION 146
Risk reduction in a system development life-cycle should be applied:

A. Mostly to the initiation phase.
B. Mostly to the development phase.
C. Mostly to the disposal phase.
D. Equally to all phases.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Risk is defined as the combination of the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability and the resulting mission impact should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by managing mission/business risk to an acceptable level.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 8).

QUESTION 147
Which of the following phases of a system development life-cycle is most concerned with maintaining proper authentication of users and processes to ensure appropriate access control decisions?

A. Development/acquisition
B. Implementation
C. Operation/Maintenance
D. Initiation

Correct Answer: C

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The operation phase of an IT system is concerned with user authentication.

Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source.

It is essential that adequate authentication be achieved in order to implement security policies and achieve security goals. Additionally, level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required.

Source: STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 15).

QUESTION 148
What can be defined as: It confirms that users' needs have been met by the supplied solution ?

A. Accreditation
B. Certification
C. Assurance
D. Acceptance

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Acceptance confirms that users' needs have been met by the supplied solution. Verification and Validation informs Acceptance by establishing the evidence – set against acceptance criteria - to determine if the solution meets the users' needs. Acceptance should also explicitly address any integration or interoperability requirements involving other equipment or systems. To enable acceptance every user and system requirement must have a 'testable' characteristic.

Accreditation is the formal acceptance of security, adequacy, authorization for operation and acceptance of existing risk. Accreditation is the formal declaration by a Designated Approving Authority (DAA) that an IS is approved to operate in a particular security mode using a prescribed set of safeguards to an acceptable level of risk.

Certification is the formal testing of security safeguards and assurance is the degree of confidence that the implemented security measures work as intended. The certification is a Comprehensive evaluation of the technical and nontechnical security features of an IS and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified ecurity requirements.

Assurance is the descriptions of the measures taken during development and evaluation of the product to assure compliance with the claimed security functionality. For example, an evaluation may require that all source code is kept in a change management system, or that full functional testing is performed. The Common Criteria provides a catalogue of these, and the requirements may vary from one evaluation to the next. The requirements for particular targets or types of products are documented in the Security Targets (ST) and Protection Profiles (PP), respectively.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 4, August 1999.

and
Official ISC2 Guide to the CISSP CBK, Second Edition, on page 211.
and
http://www.aof.mod.uk/aofcontent/tactical/randa/content/randaintroduction.htm

QUESTION 149
Which of the following statements pertaining to the security kernel is incorrect?

A. The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept.
B. The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof.
C. The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner.
D. The security kernel is an access control concept, not an actual physical component.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The reference monitor, not the security kernel is an access control concept.

The security kernel is made up of software, and firmware components that fall within the TCB and implements and enforces the reference monitor concept. The security kernel mediates all access and functions between subjects and objects. The security kernel is the core of the TCB and is the most commonly used approach to building trusted computing systems.

There are three main requirements of the security kernel:

• It must provide isolation for the processes carrying out the reference monitor concept, and the processes must be tamperproof.
• It must be invoked for every access attempt and must be impossible to circumvent. Thus, the security kernel must be implemented in a complete and foolproof way.
• It must be small enough to be able to be tested and verified in a complete and comprehensive manner.

The following answers are incorrect:

The security kernel is made up of mechanisms that fall under the TCB and implements and enforces the reference monitor concept. Is incorrect because this is the definition of the security kernel.

The security kernel must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof. Is incorrect because this is one of the three requirements that make up the security kernel.

The security kernel must be small enough to be able to be tested and verified in a complete and comprehensive manner. Is incorrect because this is one of the three requirements that make up the security kernel.

QUESTION 150
Which of the following best corresponds to the type of memory addressing where the address location that is specified in the program instruction contains the address of the final desired location?

A. Direct addressing
B. Indirect addressing
C. Indexed addressing
D. Program addressing

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Indirect addressing is when the address location that is specified in the program instruction contains the address of the final desired location. Direct addressing is when a portion of primary memory is accessed by specifying the actual address of the memory location. Indexed addressing is when the contents of the address defined in the program's instruction is added to that of an index register. Program addressing is not a defined memory addressing mode.

Source: WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 2).

QUESTION 151
Which of the following security mode of operation does NOT require all users to have the clearance for all information processed on the system?

A. Compartmented security mode
B. Multilevel security mode
C. System-high security mode
D. Dedicated security mode

Correct Answer: B

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The multilevel security mode permits two or more classification levels of information to be processed at the same time when all the users do not have the clearance of formal approval to access all the information being processed by the system.

In dedicated security mode, all users have the clearance or authorization and need-to-know to all data processed within the system.

In system-high security mode, all users have a security clearance or authorization to access the information but not necessarily a need-to-know for all the information processed on the system (only some of the data).

In compartmented security mode, all users have the clearance to access all the information processed by the system, but might not have the need-to-know and formal access approval.

Generally, Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.

The mode of operation is determined by:

The type of users who will be directly or indirectly accessing the system.
The type of data, including classification levels, compartments, and categories, that are processed on the system.
The type of levels of users, their need to know, and formal access approvals that the users will have.

Dedicated security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for ALL information on the system.
A valid need to know for ALL information on the system.

All users can access ALL data.
System high security mode

In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.

Formal access approval for ALL information on the system.
A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know.

Compartmented security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for ALL information on the system.
Formal access approval for SOME information they will access on the system.
A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know and formal access approval.

Multilevel security mode
In this mode of operation, all users must have:

Signed NDA for ALL information on the system.
Proper clearance for SOME information on the system.
Formal access approval for SOME information on the system.
A valid need to know for SOME information on the system.

All users can access SOME data, based on their need to know, clearance and formal access approval.

REFERENCES:

WALLHOFF, John, CBK#6 Security Architecture and Models (CISSP Study Guide), April 2002 (page 6).
and
http://en.wikipedia.org/wiki/Security_Modes

QUESTION 152
What prevents a process from accessing another process' data?

A. Memory segmentation B.
Process isolation
C. The reference monitor
D. Data hiding

Correct Answer: B

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Process isolation is where each process has its own distinct address space for its application code and data. In this way, it is possible to prevent each process from accessing another process' data. This prevents data leakage, or modification to the data while it is in memory. Memory segmentation is a virtual memory management mechanism. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. Data hiding, also known as information hiding, is a mechanism that makes information available at one processing level is not available at another level.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 153
What can best be defined as the sum of protection mechanisms inside the computer, including hardware, firmware and software?

A. Trusted system
B. Security kernel
C. Trusted computing base
D. Security perimeter

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Trusted Computing Base (TCB) is defined as the total combination of protection mechanisms within a computer system. The TCB includes hardware, software, and firmware. These are part of the TCB because the system is sure that these components will enforce the security policy and not violate it.

The security kernel is made up of hardware, software, and firmware components at fall within the TCB and implements and enforces the reference monitor concept.

Reference:
AIOv4 Security Models and Architecture pgs 268, 273

QUESTION 154
A trusted system does NOT involve which of the following?

A. Enforcement of a security policy.
B. Sufficiency and effectiveness of mechanisms to be able to enforce a security policy.
C. Assurance that the security policy can be enforced in an efficient and reliable manner.
D. Independently-verifiable evidence that the security policy-enforcing mechanisms are sufficient and effective.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A trusted system is one that meets its intended security requirements. It involves sufficiency and effectiveness, not necessarily efficiency, in enforcing a security policy. Put succinctly, trusted systems have (1) policy, (2) mechanism, and (3) assurance.
Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 155
What can be described as an imaginary line that separates the trusted components of the TCB from those elements that are NOT trusted?

A. The security kernel
B. The reference monitor
C. The security perimeter
D. The reference perimeter

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

The security perimeter is the imaginary line that separates the trusted components of the kernel and the Trusted Computing Base (TCB) from those elements that are not trusted. The reference monitor is an abstract machine that mediates all accesses to objects by subjects. The security kernel can be software, firmware or hardware components in a trusted system and is the actual instantiation of the reference monitor. The reference perimeter is not defined and is a distracter.

Source: HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.

QUESTION 156
A Security Kernel is defined as a strict implementation of a reference monitor mechanism responsible for enforcing a security policy. To be secure, the kernel must meet three basic conditions, what are they?

A. Confidentiality, Integrity, and Availability
B. Policy, mechanism, and assurance
C. Isolation, layering, and abstraction
D. Completeness, Isolation, and Verifiability

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A security kernel is responsible for enforcing a security policy. It is a strict implementation of a reference monitor mechanism. The architecture of a kernel operating system is typically layered, and the kernel should be at the lowest and most primitive level.

It is a small portion of the operating system through which all references to information and all changes to authorizations must pass. In theory, the kernel implements access control and information flow control between implemented objects according to the security policy.

To be secure, the kernel must meet three basic conditions:

completeness (all accesses to information must go through the kernel), isolation (the kernel itself must be protected from any type of unauthorized access), and verifiability (the kernel must be proven to meet design specifications).

The reference monitor, as noted previously, is an abstraction, but there may be a reference validator, which usually runs inside the security kernel and is responsible for performing security access checks on objects, manipulating privileges, and generating any resulting security audit messages.

A term associated with security kernels and the reference monitor is the trusted computing base (TCB). The TCB is the portion of a computer system that contains all elements of the system responsible for supporting the security policy and the isolation of objects. The security capabilities of products for use in the TCB can be verified through various evaluation criteria, such as the earlier Trusted Computer System Evaluation Criteria (TCSEC) and the current Common Criteria standard.

Many of these security terms—reference monitor, security kernel, TCB—are defined loosely by vendors for purposes of marketing literature. Thus, it is necessary for security professionals to read the small print and between the lines to fully understand what the vendor is offering in regard to security features.

TIP FOR THE EXAM:
The terms Security Kernel and Reference monitor are synonymous but at different levels.
As it was explained by Diego:

While the Reference monitor is the concept, the Security kernel is the implementation of such concept (via hardware, software and firmware means).

The two terms are the same thing, but on different levels: one is conceptual, one is "technical"

The following are incorrect answers:
Confidentiality, Integrity, and Availability
Policy, mechanism, and assurance
Isolation, layering, and abstraction

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13858-13875). Auerbach Publications. Kindle Edition.

QUESTION 157
What can best be defined as the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities, such as evaluation criteria?

A. Acceptance testing
B. Evaluation
C. Certification
D. Accreditation

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Evaluation as a general term is described as the process of independently assessing a system against a standard of comparison, such as evaluation criteria. Evaluation criterias are defined as a benchmark, standard, or yardstick against which accomplishment, conformance, performance, and suitability of an individual, hardware, software, product, or plan, as well as of risk-reward ratio is measured.

What is computer security evaluation?
Computer security evaluation is the detailed examination and testing of the security features of an IT system or product to ensure that they work correctly and effectively and do not show any logical vulnerabilities. The Security Target determines the scope of the evaluation. It includes a claimed level of Assurance that determines how rigorous the evaluation is.

Criteria
Criteria are the "standards" against which security evaluation is carried out. They define several degrees of rigour for the testing and the levels of assurance that each confers. They also define the formal requirements needed for a product (or system) to meet each Assurance level.

TCSEC
The US Department of Defense published the first criteria in 1983 as the Trusted Computer Security Evaluation Criteria (TCSEC), more popularly known as the "Orange Book". The current issue is dated 1985. The US Federal Criteria were drafted in the early 1990s as a possible replacement but were never formally adopted.

ITSEC
During the 1980s, the United Kingdom, Germany, France and the Netherlands produced versions of their own national criteria. These were harmonised and published as the Information Technology Security Evaluation Criteria (ITSEC). The current issue, Version 1.2, was published by the European Commission in June 1991. In September 1993, it was followed by the IT Security Evaluation Manual (ITSEM) which specifies the methodology to be followed when carrying out ITSEC evaluations.

Common Criteria
The Common Criteria represents the outcome of international efforts to align and develop the existing European and North American criteria. The Common Criteria project harmonises ITSEC, CTCPEC (Canadian Criteria) and US Federal Criteria (FC) into the Common Criteria for Information Technology Security Evaluation (CC) for use in evaluating products and systems and for stating security requirements in a standardised way. Increasingly it is replacing national and regional criteria with a worldwide set accepted by the International Standards Organisation (ISO15408).

The following answer were not applicable:

Certification is the process of performing a comprehensive analysis of the security features and safeguards of a system to establish the extent to which the security requirements are satisfied. Shon Harris states in her book that Certification is the comprehensive technical evaluation of the security components and their compliance for the purpose of accreditation.

Wikipedia describes it as: Certification is a comprehensive evaluation of the technical and non-technical security controls (safeguards) of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements

Accreditation is the official management decision to operate a system. Accreditation is the formal declaration by a senior agency official (Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA)) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural security controls (safeguards).
Acceptance testing refers to user testing of a system before accepting delivery.

Reference(s) used for this question:

HARE, Chris, Security Architecture and Models, Area 6 CISSP Open Study Guide, January 2002.
and
https://en.wikipedia.org/wiki/Certification_and_Accreditation
and
http://www.businessdictionary.com/definition/evaluation-criteria.html
and
http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/secevalcriteria.shtml

QUESTION 158
Which of the following is NOT a common integrity goal?

A. Prevent unauthorized users from making modifications.
B. Maintain internal and external consistency.
C. Prevent authorized users from making improper modifications.
D. Prevent paths that could lead to inappropriate disclosure.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Inappropriate disclosure is a confidentiality, not an integrity goal.
All of the other choices above are integrity goals addressed by the Clark-Wilson integrity model.

The Clark-Wilson model is an integrity model that addresses all three integrity goals:

1. prevent unauthorized users from making modifications,
2. prevent authorized users from making improper modifications, and
3. maintain internal and external consistency through auditing.

NOTE: Biba address only the first goal of integrity above

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.

QUESTION 159
When it comes to magnetic media sanitization, what difference can be made between clearing and purging information?

A. Clearing completely erases the media whereas purging only removes file headers, allowing the recovery of files.
B. Clearing renders information unrecoverable by a keyboard attack and purging renders information unrecoverable against laboratory attack.
C. They both involve rewriting the media.
D. Clearing renders information unrecoverable against a laboratory attack and purging renders information unrecoverable to a keyboard attack.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The removal of information from a storage medium is called sanitization. Different kinds of sanitization provide different levels of protection. A distinction can be made between clearing information (rendering it unrecoverable by a keyboard attack) and purging (rendering it unrecoverable against laboratory attack).

There are three general methods of purging media: overwriting, degaussing, and destruction.

There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the Automated Information System (AIS) is procured, and the procedures should be continued throughout the life cycle of the AIS.

Reference(s) use for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 26).

and
A guide to understanding Data Remanence in Automated Information Systems

QUESTION 160
What is the main issue with media reuse?

A. Degaussing
B. Data remanence
C. Media destruction
D. Purging

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The main issue with media reuse is data remanence, where residual information still resides on a media that has been erased. Degaussing, purging and destruction are ways to handle media that contains data that is no longer needed or used.
Source: WALLHOFF, John, CBK#10 Physical Security (CISSP Study Guide), April 2002 (page 5).

QUESTION 161
Which of the following should NOT be performed by an operator?

A. Implementing the initial program load
B. Monitoring execution of the system
C. Data entry
D. Controlling job flow

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Under the principle of separation of duties, an operator should not be performing data entry. This should be left to data entry personnel.

System operators represent a class of users typically found in data center environments where mainframe systems are used. They provide day-to-day operations of the mainframe environment, ensuring that scheduled jobs are running effectively and troubleshooting problems that may arise. They also act as the arms and legs of the mainframe environment, load and unloading tape and results of job print runs. Operators have elevated privileges, but less than those of system administrators. If misused, these privileges may be used to circumvent the system's security policy. As such, use of these privileges should be monitored through audit logs.

Some of the privileges and responsibilities assigned to operators include:

Implementing the initial program load: This is used to start the operating system. The boot process or initial program load of a system is a critical time for ensuring system security. Interruptions to this process may reduce the integrity of the system or cause the system to crash, precluding its availability.

Monitoring execution of the system: Operators respond to various events, to include errors, interruptions, and job completion messages.

Volume mounting: This allows the desired application access to the system and its data.

Controlling job flow: Operators can initiate, pause, or terminate programs. This may allow an operator to affect the scheduling of jobs. Controlling job flow involves the manipulation of configuration information needed by the system. Operators with the ability to control a job or application can cause output to be altered or diverted, which can threaten the confidentiality.

Bypass label processing: This allows the operator to bypass security label information to run foreign tapes (foreign tapes are those from a different data center that would not be using the same label format that the system could run). This privilege should be strictly controlled to prevent unauthorized access.

Renaming and relabeling resources: This is sometimes necessary in the mainframe environment to allow programs to properly execute. Use of this privilege should be monitored, as it can allow the unauthorized viewing of sensitive information.

Reassignment of ports and lines: Operators are allowed to reassign ports or lines. If misused, reassignment can cause program errors, such as sending sensitive output to an unsecured location. Furthermore, an incidental port may be opened, subjecting the system to an attack through the creation of a new entry point into the system.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 19367-19395). Auerbach Publications. Kindle Edition.

129
Which of the following should be performed by an operator?

A. Changing profiles
B. Approving changes
C. Adding and removal of users
D. Installing system software

Answer: D
Of the listed tasks, installing system software is the only task that should normally be performed by an operator in a properly segregated environment.
Source: MOSHER, Richard & ROTHKE, Ben, CISSP CBK Review presentation on domain 7.

QUESTION 162
Which of the following is not appropriate in addressing object reuse?

A. Degaussing magnetic tapes when they're no longer needed.
B. Deleting files on disk before reusing the space.
C. Clearing memory blocks before they are allocated to a program or data.
D. Clearing buffered pages, documents, or screens from the local memory of a terminal or printer.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

Object reuse requirements, applying to systems rated TCSEC C2 and above, are used to protect files, memory, and other objects in a trusted system from being accidentally accessed by users who are not authorized to access them. Deleting files on disk merely erases file headers in a directory structure. It does not clear data from the disk surface, thus making files still recoverable. All other options involve clearing used space, preventing any unauthorized access.

Source: RUSSEL, Deborah & GANGEMI, G.T. Sr., Computer Security Basics, O'Reilly, July 1992 (page 119).

QUESTION 163
Who of the following is responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of IT systems and data?

A. Business and functional managers
B. IT Security practitioners
C. System and information owners
D. Chief information officer

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. IT security practitioners are responsible for proper implementation of security requirements in their IT systems.
Source: STONEBURNER, Gary et al., NIST Special publication 800-30, Risk management Guide for Information Technology Systems, 2001 (page 6).

QUESTION 164
An effective information security policy should not have which of the following characteristic?

A. Include separation of duties
B. Be designed with a short- to mid-term focus
C. Be understandable and supported by all stakeholders
D. Specify areas of responsibility and authority

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
An effective information security policy should be designed with a long-term focus. All other characteristics apply.

Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 397).

QUESTION 165
Which of the following choice is NOT normally part of the questions that would be asked in regards to an organization's information security policy?

A. Who is involved in establishing the security policy?
B. Where is the organization's security policy defined?
C. What are the actions that need to be performed in case of a disaster?
D. Who is responsible for monitoring compliance to the organization's security policy?

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Actions to be performed in case of a disaster are not normally part of an information security policy but part of a Disaster Recovery Plan (DRP).

Only personnel implicated in the plan should have a copy of the Disaster Recovery Plan whereas everyone should be aware of the contents of the organization's information security policy.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Appendix B, Practice-Level Policy Considerations (page 398).

QUESTION 166
The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system is referred to as?

A. Confidentiality
B. Availability
C. Integrity
D. Reliability

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
An company security program must:

1) assure that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability;

2) protect informationcommensurate with the level of risk and magnitude ofharmresulting fromloss, misuse, unauthorized access, or modification.

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them.

The following are incorrect answers:

Confidentiality - The information requires protection from unauthorized disclosure and only the INTENDED recipient should have access to the meaning of the data either in storage or in transit.

Integrity - The information must be protected from unauthorized, unanticipated, or unintentional modification. This includes, but is not limited to:

Authenticity –A third party must be able to verify that the content of a message has not been changed in transit.

Non-repudiation – The origin or the receipt of a specific message must be verifiable by a third party.

Accountability - A security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

Reference used for this question:

RFC 2828
and
SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (page 5).

QUESTION 167
Which of the following is most concerned with personnel security?

A. Management controls
B. Operational controls
C. Technical controls
D. Human resources controls

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:

Many important issues in computer security involve human users, designers, implementers, and managers.

A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their jobs. Since operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems), personnel security is considered a form of operational control.

Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well.

Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access of misuse, facilitate detection of security violations, and support security requirements for applications and data.

Reference use for this question:

NIST SP 800-53 Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4
You can get it as a word document by clicking HERE
NIST SP 800-53 Revision 4 has superseded the document below:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Page A-18).

QUESTION 168
Which of the following would best classify as a management control?

A. Review of security controls
B. Personnel security
C. Physical and environmental protection
D. Documentation

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Management controls focus on the management of the IT security system and the management of risk for a system.

They are techniques and concerns that are normally addressed by management.
Routine evaluations and response to identified vulnerabilities are important elements of managing the risk of a system, thus considered management controls.

SECURITY CONTROLS: The management, operational, and technical controls (i.e.,safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

SECURITY CONTROL BASELINE: The set of minimum security controls defined for a low-impact, moderate-impact,or high-impact information system.

The following are incorrect answers:
Personnel security, physical and environmental protection and documentation are forms of operational controls.

Reference(s) used for this question:

http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf
and
FIPS PUB 200 at http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

QUESTION 169
Which of the following is not a form of passive attack?

A. Scavenging
B. Data diddling
C. Shoulder surfing
D. Sniffing

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Data diddling involves alteration of existing data and is extremely common. It is one of the easiest types of crimes to prevent by using access and accounting controls, supervision, auditing, separation of duties, and authorization limits. It is a form of active attack. All other choices are examples of passive attacks, only affecting confidentiality.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 10: Law, Investigation, and Ethics (page 645).

QUESTION 170
Which of the following statements pertaining to a security policy is incorrect?

A. Its main purpose is to inform the users, administrators and managers of their obligatory requirements for protecting technology and information assets.
B. It specifies how hardware and software should be used throughout the organization.

C. It needs to have the acceptance and support of all levels of employees within the organization in order for it to be appropriate and effective.
D. It must be flexible to the changing environment.

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A security policy would NOT define how hardware and software should be used throughout the organization. A standard or a procedure would provide such details but not a policy.
A security policy is a formal statement of the rules that people who are given access to anorganization's technology and information assets must abide. The policy communicates the security goals to all of the users, the administrators, and the managers. The goals will be largely determined by the following key tradeoffs: services offered versus security provided, ease of use versus security, and cost of security versus risk of loss.

The main purpose of a security policy is to inform the users, the administrators and the managers of their obligatory requirements for protecting technology and information assets.

The policy should specify the mechanisms through which these requirements can be met. Another purpose is to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy. In order for a security policy to be appropriate and effective, it needs to have the acceptance and support of all levels of employees within the organization. A good security policy must:

• Be able to be implemented through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods
• Be able to be enforced with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible • Clearly define the areas of responsibility for the users, the administrators, and the managers
• Be communicated to all once it is established

• Be flexible to the changing environment of a computer network since it is a living document

Reference(s) used for this question:

National Security Agency, Systems and Network Attack Center (SNAC),The 60 Minute Network Security Guide, February 2002, page 7.
or
A local copy is kept at:
https://www.freepracticetests.org/documents/The%2060%20Minute%20Network%20Security%20Guide.pdf

QUESTION 171
Which of the following statements pertaining to software testing is incorrect?

A. Unit testing should be addressed and considered when the modules are being designed.
B. Test data should be part of the specifications.
C. Testing should be performed with live data to cover all possible situations.
D. Test data generators can be used to systematically generate random test data that can be used to test programs.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Live or actual field data is not recommended for use in the testing procedures because both data types may not cover out of range situations and the correct outputs of the test are unknown. Live data would not be the best data to use because of the lack of anomalies and also because of the risk of exposure to your live data.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 251).

QUESTION 172
Which of the following can be defined as the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors?

A. Unit testing
B. Pilot testing
C. Regression testing
D. Parallel testing

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Regression testing is the process of rerunning a portion of the test scenario or test plan to ensure that changes or corrections have not introduced new errors. The data used in regression testing should be the same as the data used in the original test. Unit testing refers to the testing of an individual program or module. Pilot testing is a preliminary test that focuses only on specific and predetermined aspects of a system. Parallel testing is the process of feeding test data into two systems and comparing the results.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

QUESTION 173
Which of the following statements pertaining to software testing approaches is correct?

A. A bottom-up approach allows interface errors to be detected earlier.
B. A top-down approach allows errors in critical modules to be detected earlier.
C. The test plan and results should be retained as part of the system's permanent documentation.
D. Black box testing is predicated on a close examination of procedural detail.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A bottom-up approach to testing begins testing of atomic units, such as programs or modules, and works upwards until a complete system testing has taken place. It allows errors in critical modules to be found early. A top-down approach allows for early detection of interface errors and raises confidence in the system, as programmers and users actually see a working system. White box testing is predicated on a close examination of procedural detail. Black box testing examines some aspect of the system with little regard for the internal logical structure of the software.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

Top Down Testing: An approach to integration testing where the component at the top of the component hierarchy is tested first, with lower level components being simulated by stubs. Tested components are then used to test lower level components. The process is repeated until the lowest level components have been tested.

Bottom Up Testing: An approach to integration testing where the lowest level components are tested first, then used to facilitate the testing of higher level components. The process is repeated until the component at the top of the hierarchy is tested.

Black Box Testing: Testing based on an analysis of the specification of a piece of software without reference to its internal workings. The goal is to test how well the component conforms to the published requirements for the component.

QUESTION 174
Which of the following test makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems?

A. Recovery testing
B. Security testing
C. Stress/volume testing
D. Interface testing

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Security testing makes sure the modified or new system includes appropriate access controls and does not introduce any security holes that might compromise other systems.

Recovery testing checks the system's ability to recover after a software or hardware failure.

Stress/volume testing involves testing an application with large quantities of data in order to evaluate performance during peak hours.
Interface testing evaluates the connection of two or more components that pass information from one area to another.

Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 6: Business Application System Development, Acquisition, Implementation and Maintenance (page 300).

QUESTION 175
Which of the following phases of a software development life cycle normally addresses Due Care and Due Diligence?

A. Implementation
B. System feasibility
C. Product design
D. Software plans and requirements

Correct Answer: D

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The software plans and requirements phase addresses threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).

System Feasibility is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts.

Product design is incorrect because it deals with incorporating security specifications, adjusting test plans and data, determining access controls, design documentation, evaluating encryption options, and verification.

Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

QUESTION 176
Which of the following phases of a software development life cycle normally incorporates the security specifications, determines access controls, and evaluates encryption options?

A. Detailed design
B. Implementation
C. Product design
D. Software plans and requirements

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Product design phase deals with incorporating security specifications, adjusting test plans and data, determining access controls, design documentation, evaluating encryption options, and verification.

Implementation is incorrect because it deals with Installing security software, running the system, acceptance testing, security software testing, and complete documentation certification and accreditation (where necessary).

Detailed design is incorrect because it deals with information security policy, standards, legal issues, and the early validation of concepts. software plans and requirements is incorrect because it deals with addressesing threats, vulnerabilities, security requirements, reasonable care, due diligence, legal liabilities, cost/benefit analysis, level of protection desired, test plans.

Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Security Life Cycle Components, Figure 7.5 (page 346).

145
At which of the basic phases of the System Development Life Cycle are security requirements formalized?

A. Disposal
B. System Design Specifications
C. Development and Implementation
D. Functional Requirements Definition

Answer: D
During the Functional Requirements Definition the project management and systems development teams will conduct a comprehensive analysis of current and possible future functional requirements to ensure that the new system will meet end-user needs. The teams also review the documents from the project initiation phase and make any revisions or updates as needed. For smaller projects, this phase is often subsumed in the project initiation phase. At this point security requirements should be formalized.

The Development Life Cycle is a project management tool that can be used to plan, execute, and control a software development project usually called the Systems Development Life Cycle (SDLC).

The SDLC is a process that includes systems analysts, software engineers, programmers, and end users in the project design and development. Because there is no industry-wide SDLC, an organization can use any one, or a combination of SDLC methods.

The SDLC simply provides a framework for the phases of a software development project from defining the functional requirements to implementation. Regardless of the method used, the SDLC outlines the essential phases, which can be shown together or as separate elements. The model chosen should be based on the project.

For example, some models work better with long-term, complex projects, while others are more suited for short-term projects. The key element is that a formalized SDLC is utilized.

The number of phases can range from three basic phases (concept, design, and implement) on up.

The basic phases of SDLC are:

Project initiation and planning
Functional requirements definition
System design specifications
Development and implementation
Documentation and common program controls
Testing and evaluation control, (certification and accreditation)
Transition to production (implementation)

The system life cycle (SLC) extends beyond the SDLC to include two additional phases:

Operations and maintenance support (post-installation)
Revisions and system replacement

System Design Specifications
This phase includes all activities related to designing the system and software. In this phase, the system architecture, system outputs, and system interfaces are designed. Data input, data flow, and output requirements are established and security features are designed, generally based on the overall security architecture for the company.

Development and Implementation
During this phase, the source code is generated, test scenarios and test cases are developed, unit and integration testing is conducted, and the program and system are documented for maintenance and for turnover to acceptance testing and production. As well as general care for software quality, reliability, and consistency of operation, particular care should be taken to ensure that the code is analyzed to eliminate common vulnerabilities that might lead to security exploits and other risks.

Documentation and Common Program Controls
These are controls used when editing the data within the program, the types of logging the program should be doing, and how the program versions should be stored. A large number of such controls may be needed, see the reference below for a full list of controls.

Acceptance
In the acceptance phase, preferably an independent group develops test data and tests the code to ensure that it will function within the organization’s environment and that it meets all the functional and security requirements. It is essential that an independent group test the code during all applicable stages of development to prevent a separation of duties issue. The goal of security testing is to ensure that the application meets its security requirements and specifications. The security

testing should uncover all design and implementation flaws that would allow a user to violate the software security policy and requirements. To ensure test validity, the application should be tested in an environment that simulates the production environment. This should include a security certification package and any user documentation.

Certification and Accreditation (Security Authorization)
Certification is the process of evaluating the security stance of the software or system against a predetermined set of security standards or policies. Certification also examines how well the system performs its intended functional requirements. The certification or evaluation document should contain an analysis of the technical and nontechnical security features and countermeasures and the extent to which the software or system meets the security requirements for its mission and operational environment.

Transition to Production (Implementation)
During this phase, the new system is transitioned from the acceptance phase into the live production environment. Activities during this phase include obtaining security accreditation; training the new users according to the implementation and training schedules; implementing the system, including installation and data conversions; and, if necessary, conducting any parallel operations.

Revisions and System Replacement
As systems are in production mode, the hardware and software baselines should be subject to periodic evaluations and audits. In some instances, problems with the application may not be defects or flaws, but rather additional functions not currently developed in the application. Any changes to the application must follow the same SDLC and be recorded in a change management system. Revision reviews should include security planning and procedures to avoid future problems. Periodic application audits should be conducted and include documenting security incidents when problems occur. Documenting system failures is a valuable resource for justifying future system enhancements.

Below you have the phases used by NIST in it's 800-63 Revision 2 document

As noted above, the phases will vary from one document to another one. For the purpose of the exam use the list provided in the official ISC2 Study book which is presented in short form above. Refer to the book for a more detailed description of activities at each of the phases of the SDLC.

However, all references have very similar steps being used. As mentioned in the official book, it could be as simple as three phases in it's most basic version (concept, design, and implement) or a lot more in more detailed versions of the SDLC. The key thing is to make use of an SDLC.

SDLC phases

Reference(s) used for this question:

NIST SP 800-64 Revision 2 at http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition: Software Development Security ((ISC)2 Press) (Kindle Locations 134-157). Auerbach Publications. Kindle Edition.

QUESTION 177
Which of the following is less likely to be included in the change control sub-phase of the maintenance phase of a software product?

A. Estimating the cost of the changes requested
B. Recreating and analyzing the problem
C. Determining the interface that is presented to the user
D. Establishing the priorities of requests

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Change control sub-phase includes Recreating and analyzing the problem, Determining the interface that is presented to the user, and Establishing the priorities of requests.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 252).

QUESTION 178
What is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity?

A. Polyinstantiation
B. Inference
C. Aggregation
D. Data mining

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Aggregation is the act of obtaining information of a higher sensitivity by combining information from lower levels of sensitivity.

The incorrect answers are:

Polyinstantiation is the development of a detailed version of an object from another object using different values in the new object.

Inference is the ability of users to infer or deduce information about data at sensitivity levels for which they do not have access privilege.

Data mining refers to searching through a data warehouse for data correlations.

Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 261).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Database Security Issues (page 358).

QUESTION 179
Which expert system operating mode allows determining if a given hypothesis is valid?

A. Blackboard
B. Lateral chaining
C. Forward chaining
D. Backward chaining

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Backward-chaining mode - the expert system backtracks to determine if a given hypothesis is valid. Backward-chaining is generally used when there are a large number of possible solutions relative to the number of inputs.

Incorrect answers are:
In a forward-chaining mode, the expert system acquires information and comes to a conclusion based on that information. Forward-chaining is the reasoning approach that can be used when there is a small number of solutions relative to the number of inputs.

Blackboard is an expert system-reasoning methodology in which a solution is generated by the use of a virtual blackboard, wherein information or potential solutions are placed on the blackboard by a plurality of individuals or expert knowledge sources. As more information is placed on the blackboard in an iterative process, a solution is generated.

Lateral-chaining mode - No such expert system mode.
Sources:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 259).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 7: Expert Systems (page 354).

QUESTION 180
Why does compiled code pose more of a security risk than interpreted code?

A. Because malicious code can be embedded in compiled code and be difficult to detect.
B. If the executed compiled code fails, there is a chance it will fail insecurely.
C. Because compilers are not reliable.
D. There is no risk difference between interpreted code and compiled code.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
From a security standpoint, a compiled program is less desirable than an interpreted one because malicious code can be resident somewhere in the compiled code, and it is difficult to detect in a very large program.

Incorrect answers:

There is a risk difference between interpreted code and compiled code.

Compilers are reliable.
The risk of a program failing insecurely is not the result of compiled or interpreted code.

Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 263).
KRUTZ, Ronald & VINES, Russel, The CISSP Prep Guide: Gold Edition, Wiley Publishing Inc., 2003, Chapter 2: Security Architecture and Models, Software (page 258).

QUESTION 181
Which software development model is actually a meta-model that incorporates a number of the software development models?

A. The Waterfall model
B. The modified Waterfall model
C. The Spiral model
D. The Critical Path Model (CPM)

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The spiral model is actually a meta-model that incorporates a number of the software development models. This model depicts a spiral that incorporates the various phases of software development. The model states that each cycle of the spiral involves the same series of steps for each part of the project. CPM refers to the Critical Path Methodology.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 7: Applications and Systems Development (page 246).

QUESTION 182
Which of the following is used in database information security to hide information?

A. Inheritance
B. Polyinstantiation
C. Polymorphism

D. Delegation

Correct Answer: B
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Polyinstantiation enables a relation to contain multiple tuples with the same primary keys with each instance distinguished by a security level. When this information is inserted into a database, lower-level subjects need to be restricted from this information. Instead of just restricting access, another set of data is created to fool the lower-level subjects into thinking that the information actually means something else.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 727).

QUESTION 183
Which of the following computer design approaches is based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle?

A. Pipelining
B. Reduced Instruction Set Computers (RISC)
C. Complex Instruction Set Computers (CISC)
D. Scalar processors

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Complex Instruction Set Computer (CISC) uses instructions that perform many operations per instruction. It was based on the fact that in earlier technologies, the instruction fetch was the longest part of the cycle. Therefore, by packing more operations into an instruction, the number of fetches could be reduced. Pipelining involves overlapping the steps of different instructions to increase the performance in a computer. Reduced Instruction Set Computers (RISC) involve simpler instructions that require fewer clock cycles to execute. Scalar processors are processors that execute one instruction at a time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 188).

QUESTION 184
What is used to protect programs from all unauthorized modification or executional interference?

A. A protection domain
B. A security perimeter
C. Security labels

D. Abstraction

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A protection domain consists of the execution and memory space assigned to each process. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executional interference. The security perimeter is the boundary that separates the Trusted Computing Base (TCB) from the remainder of the system. Security labels are assigned to resources to denote a type of classification. Abstraction is a way to protect resources in the fact that it involves viewing system components at a high level and ignoring its specific details, thus performing information hiding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 193).

QUESTION 185
What is called a system that is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it?

A. A fail safe system
B. A fail soft system
C. A fault-tolerant system
D. A failover system

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A fault-tolerant system is capable of detecting that a fault has occurred and has the ability to correct the fault or operate around it. In a fail-safe system, program execution is terminated, and the system is protected from being compromised when a hardware or software failure occurs and is detected. In a fail-soft system, when a hardware or software failure occurs and is detected, selected, non-critical processing is terminated. The term failover refers to switching to a duplicate "hot" backup component in real-time when a hardware or software failure occurs, enabling processing to continue.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 196).

QUESTION 186
What is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept?

A. The reference monitor

B. Protection rings
C. A security kernel
D. A protection domain

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A security kernel is defined as the hardware, firmware and software elements of a trusted computing base that implement the reference monitor concept. A reference monitor is a system component that enforces access controls on an object. A protection domain consists of the execution and memory space assigned to each process. The use of protection rings is a scheme that supports multiple protection domains.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architecture and Models (page 194).

QUESTION 187
Which of the following rules is least likely to support the concept of least privilege?

A. The number of administrative accounts should be kept to a minimum.
B. Administrators should use regular accounts when performing routine operations like reading mail.
C. Permissions on tools that are likely to be used by hackers should be as restrictive as possible.
D. Only data to and from critical systems and applications should be allowed through the firewall.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation
Explanation/Reference:
Only data to and from critical systems and applications should be allowed through the firewall is a detractor. Critical systems or applications do not necessarily need to have traffic go through a firewall. Even if they did, only the minimum required services should be allowed. Systems that are not deemed critical may also need to have traffic go through the firewall.

Least privilege is a basic tenet of computer security that means users should be given only those rights required to do their jobs or tasks. Least privilege is ensuring that you have the minimum privileges necessary to do a task. An admin NOT using his admin account to check email is a clear example of this.

Reference(s) used for this question:
National Security Agency, Systems and Network Attack Center (SNAC), The 60 Minute Network Security Guide, February 2002, page 9.

QUESTION 188

Which of the following is an unintended communication path that is NOT protected by the system's normal security mechanisms?

A. A trusted path
B. A protection domain
C. A covert channel
D. A maintenance hook

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
A covert channel is an unintended communication path within a system, therefore it is not protected by the system's normal security mechanisms. Covert channels are a secret way to convey information.

Covert channels are addressed from TCSEC level B2.

The following are incorrect answers:

A trusted path is the protected channel that allows a user to access the Trusted Computing Base (TCB) without being compromised by other processes or users.

A protection domain consists of the execution and memory space assigned to each process.

A maintenance hook is a hardware or software mechanism that was installed to permit system maintenance and to bypass the system's security protections.

Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 6: Operations Security (page 219).

QUESTION 189
Which of the following is used to interrupt the opportunity to use or perform collusion to subvert operation for fraudulent purposes?

A. Key escrow
B. Rotation of duties
C. Principle of need-to-know
D. Principle of least privilege

Correct Answer: B

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Job rotations reduce the risk of collusion of activities between individuals. Companies with individuals working with sensitive information or systems where there might be the opportunity for personal gain through collusion can benefit by integrating job rotation with segregation of duties. Rotating the position may uncover activities that the individual is performing outside of the normal operating procedures, highlighting errors or fraudulent behavior.

Rotation of duties is a method of reducing the risk associated with a subject performing a (sensitive) task by limiting the amount of time the subject is assigned to perform the task before being moved to a different task.

The following are incorrect answers:
Key escrow is related to the protection of keys in storage by splitting the key in pieces that will be controlled by different departments. Key escrow is the process of ensuring a third party maintains a copy of a private key or key needed to decrypt information. Key escrow also should be considered mandatory for most organization's use of cryptography as encrypted information belongs to the organization and not the individual; however often an individual's key is used to encrypt the information.

Separation of duties is a basic control that prevents or detects errors and irregularities by assigning responsibility for different parts of critical tasks to separate individuals, thus limiting the effect a single person can have on a system. One individual should not have the capability to execute all of the steps of a particular process. This is especially important in critical business areas, where individuals may have greater access and capability to modify, delete, or add data to the system. Failure to separate duties could result in individuals embezzling money from the company without the involvement of others.

The need-to-know principle specifies that a person must not only be cleared to access classified or other sensitive information, but have requirement for such information to carry out assigned job duties. Ordinary or limited user accounts are what most users are assigned. They should be restricted only to those privileges that are strictly required, following the principle of least privilege. Access should be limited to specific objects following the principle of need-to-know.

The principle of least privilege requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. Least privilege refers to granting users only the accesses that are required to perform their job functions. Some employees will require greater access than others based upon their job functions. For example, an individual performing data entry on a mainframe system may have no need for Internet access or the ability to run reports regarding the information that they are entering into the system. Conversely, a supervisor may have the need to run reports, but should not be provided the capability to change information in the database.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10628-10631). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10635-10638). Auerbach Publications. Kindle Edition. and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10693-10697). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16338-16341). Auerbach Publications. Kindle Edition.

QUESTION 190
Which of the following is best defined as an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards?

A. Certification
B. Declaration
C. Audit
D. Accreditation

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Accreditation: is an administrative declaration by a designated authority that an information system is approved to operate in a particular security configuration with a prescribed set of safeguards. It is usually based on a technical certification of the system's security mechanisms.

Certification: Technical evaluation (usually made in support of an accreditation action) of an information system\'s security features and other safeguards to establish the extent to which the system\'s design and implementation meet specified security requirements.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 191

Which of the following is best defined as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it?

A. Aggregation
B. Inference
C. Clustering
D. Collision

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Internet Security Glossary (RFC2828) defines aggregation as a circumstance in which a collection of information items is required to be classified at a higher security level than any of the individual items that comprise it.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 192
Which of the following best defines add-on security?

A. Physical security complementing logical security measures.
B. Protection mechanisms implemented as an integral part of an information system.
C. Layer security.
D. Protection mechanisms implemented after an information system has become operational.

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Internet Security Glossary (RFC2828) defines add-on security as "The retrofitting of protection mechanisms, implemented by hardware or software, after the [automatic data processing] system has become operational."
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 193
Which of the following is best defined as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in a system?

A. Fail proof
B. Fail soft
C. Fail safe
D. Fail Over

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
NOTE: This question is referring to a system which is Logical/Technical, so it is in the context of a system that you must choose the right answer. This is very important to read the question carefully and to identify the context whether it is in the Physical world or in the Technical/Logical world.

RFC 2828 (Internet Security Glossary) defines fail safe as a mode of system termination that automatically leaves system processes and components in a secure state when a failure occurs or is detected in the system.

A secure state means in the Logical/Technical world that no access would be granted or no packets would be allowed to flow through the system inspecting the packets such as a firewall for example.

If the question would have made reference to a building or something specific to the Physical world then the answer would have been different. In the Physical World everything becomes open and full access would be granted. See the valid choices below for the Physical context.

Fail-safe in the physical security world is when doors are unlocked automatically in case of emergency. Used in environment where humans work around. As human safety is prime concern during Fire or other hazards.

The following were all wrong choices:

Fail-secure in the physical security world is when doors are locked automatically in case of emergency. Can be in an area like Cash Locker Room provided there should be alternative manually operated exit door in case of emergency.

Fail soft is selective termination of affected non-essential system functions and processes when a failure occurs or is detected in the system.

Fail Over is a redundancy mechanism and does not apply to this question.
There is a great post within the CCCure Forums on this specific Q:

saintrockz who is a long term contributor to the forums did outstanding research and you have the results below. The CCCure forum is a gold mine where thousands of Qs related to the CBK have been discussed.

According to the Official ISC2 Study Guide (OIG):

Fault Tolerance is defined as built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults. It means a system can operate in the presence of hardware component failures. A single component failure in a fault-tolerant system will not cause a system interruption because the alternate component will take over the task transparently. As the cost of components continues to drop, and the demand for system availability increases, many non-fault-tolerant systems have redundancy built-in at the subsystem level. As a result, many non-fault-tolerant systems can tolerate hardware faults - consequently, the line between a fault-tolerant system and a non-fault-tolerant system becomes increasingly blurred.

According to Common Criteria:
Fail Secure - Failure with preservation of secure state, which requires that the TSF (TOE security functions) preserve a secure state in the face of the identified failures.

Acc. to The CISSP Prep Guide, Gold Ed.:
Fail over - When one system/application fails, operations will automatically switch to the backup system.
Fail safe - Pertaining to the automatic protection of programs and/or processing systems to maintain safety when a hardware or software failure is detected in a system.
Fail secure - The system preserves a secure state during and after identified failures occur.
Fail soft - Pertaining to the selective termination of affected non-essential processing when a hardware or software failure is detected in a system.

Acc. to CISSP for Dummies:
Fail closed - A control failure that results all accesses blocked.
Fail open - A control failure that results in all accesses permitted.
Failover - A failure mode where, if a hardware or software failure is detected, the system automatically transfers processing to a hot backup component, such as a clustered server.
Fail-safe - A failure mode where, if a hardware or software failure is detected, program execution is terminated, and the system is protected from compromise. Fail-soft (or resilient) - A failure mode where, if a hardware or software failure is detected, certain, noncritical processing is terminated, and the computer or network continues to function in a degraded mode.
Fault-tolerant - A system that continues to operate following failure of a computer or network component.

It's good to differentiate this concept in Physical Security as well:

Fail-safe
• Door defaults to being unlocked
• Dictated by fire codes

Fail-secure
• Door defaults to being locked

Reference(s) used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 194
The preliminary steps to security planning include all of the following EXCEPT which of the following?

A. Establish objectives.
B. List planning assumptions.
C. Establish a security audit function.
D. Determine alternate courses of action

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The keyword within the question is: preliminary

This means that you are starting your effort, you cannot audit if your infrastructure is not even in place.

Reference used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 195
Step-by-step instructions used to satisfy control requirements is called a:

A. policy
B. standard
C. guideline
D. procedure

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 196

One purpose of a security awareness program is to modify:

A. employee's attitudes and behaviors towards enterprise's security posture
B. management's approach towards enterprise's security posture
C. attitudes of employees with sensitive data
D. corporate attitudes about safeguarding data

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Answer: security awareness training is to modify employees behaviour and attitude towards towards enterprise's security posture.

Security-awareness training is performed to modify employees' behavior and attitude toward security. This can best be achieved through a formalized process of security-awareness training.

It is used to increase the overall awareness of security throughout the company. It is targeted to every single employee and not only to one group of users.

Unfortunately you cannot apply a patch to a human being, the only thing you can do is to educate employees and make them more aware of security issues and threats. Never underestimate human stupidity.

Reference(s) used for this question:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
also see:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 130). McGraw-Hill. Kindle Edition.

QUESTION 197
Whose role is it to assign classification level to information?

A. Security Administrator
B. User
C. Owner
D. Auditor

Correct Answer: C

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The Data/Information Owner is ultimately responsible for the protection of the data. It is the Data/Information Owner that decides upon the classifications of that data they are responsible for.

The data owner decides upon the classification of the data he is responsible for and alters that classification if the business need arises.

The following answers are incorrect:

Security Administrator. Is incorrect because this individual is responsible for ensuring that the access right granted are correct and support the polices and directives that the Data/Information Owner defines.

User. Is Incorrect because the user uses/access the data according to how the Data/Information Owner defined their access.

Auditor. Is incorrect because the Auditor is responsible for ensuring that the access levels are appropriate. The Auditor would verify that the Owner classified the data properly.

References:
CISSP All In One Third Edition, Shon Harris, Page 121

QUESTION 198
Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

A. Limiting the local access of operations personnel
B. Job rotation of operations personnel
C. Management monitoring of audit logs
D. Enforcing regular password changes

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.
Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be force to use collusion to defeat those security mechanism. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 199
What is the most secure way to dispose of information on a CD-ROM?

A. Sanitizing
B. Physical damage
C. Degaussing
D. Physical destruction

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
First you have to realize that the question is specifically talking about a CDROM. The information stored on a CDROM is not in electro magnetic format, so a degausser woud be inneffective.

You cannot sanitize a CDROM but you might be able to sanitize a RW/CDROM. A CDROM is a write once device and cannot be overwritten like a hard disk or other magnetic device.

Physical Damage would not be enough as information could still be extracted in a lab from the undamaged portion of the media or even from the pieces after the physical damage has been done.

Physical Destruction using a shredder, your microwave oven, melting it, would be very effective and the best choice for a non magnetic media such as a CDROM. Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 200
The Reference Validation Mechanism that ensures the authorized access relationships between subjects and objects is implementing which of the following concept:

A. The reference monitor.
B. Discretionary Access Control.
C. The Security Kernel.

D. Mandatory Access Control.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
The reference monitor concept is an abstract machine that ensures that all subjects have the necessary access rights before accessing objects. Therefore, the kernel will mediates all accesses to objects by subjects and will do so by validating through the reference monitor concept.

The kernel does not decide whether or not the access will be granted, it will be the Reference Monitor which is a subset of the kernel that will say YES or NO.

All access requests will be intercepted by the Kernel, validated through the reference monitor, and then access will either be denied or granted according to the request and the subject privileges within the system.

1. The reference monitor must be small enough to be full tested and valided
2. The Kernel must MEDIATE all access request from subjects to objects
3. The processes implementing the reference monitor must be protected
4. The reference monitor must be tamperproof

The following answers are incorrect:

The security kernel is the mechanism that actually enforces the rules of the reference monitor concept.

The other answers are distractors.

Shon Harris, All In One, 5th Edition, Security Architecture and Design, Page 330 also see http://en.wikipedia.org/wiki/Reference_monitor

QUESTION 201
Which of the following describes a logical form of separation used by secure computing systems?

A. Processes use different levels of security for input and output devices.
B. Processes are constrained so that each cannot access objects outside its permitted domain.
C. Processes conceal data and computations to inhibit access by outside processes.
D. Processes are granted access based on granularity of controlled objects.

Correct Answer: B

Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 202
What security problem is most likely to exist if an operating system permits objects to be used sequentially by multiple users without forcing a refresh of the objects?

A. Disclosure of residual data.
B. Unauthorized obtaining of a privileged execution state.
C. Denial of service through a deadly embrace.
D. Data leakage through covert channels.

Correct Answer: A
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
This question is asking you to consider the effects of object reuse. Object reuse is "reassigning to subject media that previously contained information. Object reuse is a security concern because if insufficient measures were taken to erase the information on the media, the information may be disclosed to unauthorized personnel."

This concept relates to Security Architecture and Design, because it is in level C2: Controlled Access Protection, of the Orange Book, where "The object reuse concept must be invoked, meaning that any medium holding data must not contain any remnants of information after it is release for another subject to use."

REFERENCE:

AIO Version 5 (Shon Harris), page 360
and
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 203
At what stage of the applications development process should the security department become involved?

A. Prior to the implementation
B. Prior to systems testing

C. During unit testing
D. During requirements development

Correct Answer: D
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 204
In what way could Java applets pose a security threat?

A. Their transport can interrupt the secure distribution of World Wide Web pages over the Internet by removing SSL and S-HTTP
B. Java interpreters do not provide the ability to limit system access that an applet could have on a client system.
C. Executables from the Internet may attempt an intentional attack when they are downloaded on a client system.
D. Java does not check the bytecode at runtime or provide other safety mechanisms for program isolation from the client system.

Correct Answer: C
Section: Security Operation Adimnistration
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 205
Which of the following is needed for System Accountability?

A. Audit mechanisms.
B. Documented design as laid out in the Common Criteria.
C. Authorization.
D. Formal verification of system design.

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Is a means of being able to track user actions. Through the use of audit logs and other tools the user actions are recorded and can be used at a later date to verify what actions were performed.

Accountability is the ability to identify users and to be able to track user actions.

The following answers are incorrect:

Documented design as laid out in the Common Criteria. Is incorrect because the Common Criteria is an international standard to evaluate trust and would not be a factor in System Accountability.

Authorization. Is incorrect because Authorization is granting access to subjects, just because you have authorization does not hold the subject accountable for their actions.

Formal verification of system design. Is incorrect because all you have done is to verify the system design and have not taken any steps toward system accountability.

References:

OIG CBK Glossary (page 778)

QUESTION 206
A timely review of system access audit records would be an example of which of the basic security functions?

A. avoidance
B. deterrence
C. prevention
D. detection

Correct Answer: D
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
By reviewing system logs you can detect events that have occured.

The following answers are incorrect:

avoidance. This is incorrect, avoidance is a distractor. By reviewing system logs you have not avoided anything. deterrence. This is incorrect because system logs are a history of past events. You cannot deter something that has already occurred. prevention. This is incorrect because system logs are a history of past events. You cannot prevent something that has already occurred.

QUESTION 207
Which of the following would assist the most in Host Based intrusion detection?

A. audit trails.
B. access control lists.
C. security clearances
D. host-based authentication

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
To assist in Intrusion Detection you would review audit logs for access violations.

The following answers are incorrect:

access control lists. This is incorrect because access control lists determine who has access to what but do not detect intrusions.

security clearances. This is incorrect because security clearances determine who has access to what but do not detect intrusions.

host-based authentication. This is incorrect because host-based authentication determine who have been authenticated to the system but do not dectect intrusions.

QUESTION 208
Who should measure the effectiveness of Information System security related controls in an organization?

A. The local security specialist
B. The business manager
C. The systems auditor
D. The central security manager

Correct Answer: C

Section: Analysis and Monitoring
Explanation

Explanation/Reference:
It is the systems auditor that should lead the effort to ensure that the security controls are in place and effective. The audit would verify that the controls comply with polices, procedures, laws, and regulations where applicable. The findings would provide these to senior management.

The following answers are incorrect:
the local security specialist. Is incorrect because an independent review should take place by a third party. The security specialist might offer mitigation strategies but it is the auditor that would ensure the effectiveness of the controls

the business manager. Is incorrect because the business manager would be responsible that the controls are in place, but it is the auditor that would ensure the effectiveness of the controls.

the central security manager. Is incorrect because the central security manager would be responsible for implementing the controls, but it is the auditor that is responsibe for ensuring their effectiveness.

QUESTION 209
In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

A. The transactions should be dropped from processing.
B. The transactions should be processed after the program makes adjustments.
C. The transactions should be written to a report and reviewed.
D. The transactions should be corrected and reprocessed.

Correct Answer: C
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

As explained in the ISC2 OIG:
OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transactionoriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change realtime data.

OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.

The security concerns for OLTP systems are concurrency and atomicity.

Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.

Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete.

OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the transaction logs.

Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:
Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions.

OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY
In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.

The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR
neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY
Database concurrency controls ensure that transactions occur in an ordered fashion.

The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read http://en.wikipedia.org/wiki/ACID for more details on the ACID test.

Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms.

Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.

The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

References:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition. and
http://en.wikipedia.org/wiki/Online_transaction_processing
and

http://databases.about.com/od/administration/g/concurrency.htm

QUESTION 210
Who can best decide what are the adequate technical security controls in a computer-based application system in regards to the protection of the data being used, the criticality of the data, and it's sensitivity level ?

A. System Auditor
B. Data or Information Owner
C. System Manager
D. Data or Information user

Correct Answer: B
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
The data or information owner also referred to as "Data Owner" would be the best person. That is the individual or officer who is ultimately responsible for the protection of the information and can therefore decide what are the adequate security controls according to the data sensitivity and data criticality. The auditor would be the best person to determine the adequacy of controls and whether or not they are working as expected by the owner.

The function of the auditor is to come around periodically and make sure you are doing what you are supposed to be doing. They ensure the correct controls are in place and are being maintained securely. The goal of the auditor is to make sure the organization complies with its own policies and the applicable laws and regulations.

Organizations can have internal auditors and/ or external auditors. The external auditors commonly work on behalf of a regulatory body to make sure compliance is being met. For example CobiT, which is a model that most information security auditors follow when evaluating a security program. While many security professionals fear and dread auditors, they can be valuable tools in ensuring the overall security of the organization. Their goal is to find the things you have missed and help you understand how to fix the problem.

The Official ISC2 Guide (OIG) says:
IT auditors determine whether users, owners, custodians, systems, and networks are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction, and other requirements placed on systems. The auditors provide independent assurance to the management on the appropriateness of the security controls. The auditor examines the information systems and determines whether they are designed, configured, implemented, operated, and managed in a way ensuring that the organizational objectives are being achieved. The auditors provide top company management with an independent view of the controls and their effectiveness.

Example:

Bob is the head of payroll. He is therefore the individual with primary responsibility over the payroll database, and is therefore the information/data owner of the payroll database. In Bob's department, he has Sally and Richard working for him. Sally is responsible for making changes to the payroll database, for example if someone is hired or gets a raise. Richard is only responsible for printing paychecks. Given those roles, Sally requires both read and write access to the payroll database, but Richard requires only read access to it. Bob communicates these requirements to the system administrators (the "information/data custodians") and they set the file permissions for Sally's and Richard's user accounts so that Sally has read/write access, while Richard has only read access.

So in short Bob will determine what controls are required, what is the sensitivily and criticality of the Data. Bob will communicate this to the custodians who will implement the requirements on the systems/DB. The auditor would assess if the controls are in fact providing the level of security the Data Owner expects within the systems/DB. The auditor does not determine the sensitivity of the data or the crititicality of the data.

The other answers are not correct because:
A "system auditor" is never responsible for anything but auditing... not actually making control decisions but the auditor would be the best person to determine the adequacy of controls and then make recommendations.

A "system manager" is really just another name for a system administrator, which is actually an information custodian as explained above.

A "Data or information user" is responsible for implementing security controls on a day-to-day basis as they utilize the information, but not for determining what the controls should be or if they are adequate.

References:
Official ISC2 Guide to the CISSP CBK, Third Edition , Page 477

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Information Security Governance and Risk Management ((ISC)2 Press) (Kindle Locations 294-298). Auerbach Publications. Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 3108-3114).

Information Security Glossary
Responsibility for use of information resources

QUESTION 211
Attributable data should be:

A. always traced to individuals responsible for observing and recording the data

B. sometimes traced to individuals responsible for observing and recording the data
C. never traced to individuals responsible for observing and recording the data
D. often traced to individuals responsible for observing and recording the data

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
As per FDA data should be attributable, original, accurate, contemporaneous and legible. In an automated system attributability could be achieved by a computer system designed to identify individuals responsible for any input.
Source: U.S. Department of Health and Human Services, Food and Drug Administration, Guidance for Industry - Computerized Systems Used in Clinical Trials, April 1999, page 1.

QUESTION 212
Which of the following best describes signature-based detection?

A. Compare source code, looking for events or sets of events that could cause damage to a system or network.
B. Compare system activity for the behaviour patterns of new attacks.
C. Compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack.
D. Compare network nodes looking for objects or sets of objects that match a predefined pattern of objects that may describe a known attack.

Correct Answer: C
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Misuse detectors compare system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. As the patterns corresponding to known attacks are called signatures, misuse detection is sometimes called "signature-based detection."

The most common form of misuse detection used in commercial products specifies each pattern of events corresponding to an attack as a separate signature. However, there are more sophisticated approaches to doing misuse detection (called "state-based" analysis techniques) that can leverage a single signature to detect groups of attacks.

Reference:

Old Document:
BACE, Rebecca & MELL, Peter, NIST Special Publication 800-31 on Intrusion Detection Systems, Page 16.

The publication above has been replaced by 800-94 on page 2-4

The Updated URL is: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

QUESTION 213
Which of the following is used to monitor network traffic or to monitor host audit logs in real time to determine violations of system security policy that have taken place?

A. Intrusion Detection System
B. Compliance Validation System
C. Intrusion Management System (IMS)
D. Compliance Monitoring System

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
An Intrusion Detection System (IDS) is a system that is used to monitor network traffic or to monitor host audit logs in order to determine if any violations of an organization's system security policy have taken place.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 214
Which of the following monitors network traffic in real time?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
This type of IDS is called a network-based IDS because monitors network traffic in real time.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 215
A host-based IDS is resident on which of the following?

A. On each of the critical hosts

B. decentralized hosts
C. central hosts
D. bastion hosts

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
A host-based IDS is resident on a host and reviews the system and event logs in order to detect an attack on the host and to determine if the attack was successful. All critical serves should have a Host Based Intrusion Detection System (HIDS) installed. As you are well aware, network based IDS cannot make sense or detect pattern of attacks within encrypted traffic. A HIDS might be able to detect such attack after the traffic has been decrypted on the host. This is why critical servers should have both NIDS and HIDS.

FROM WIKIPEDIA:
A HIDS will monitor all or part of the dynamic behavior and of the state of a computer system. Much as a NIDS will dynamically inspect network packets, a HIDS might detect which program accesses what resources and assure that (say) a word-processor hasn\'t suddenly and inexplicably started modifying the system password-database. Similarly a HIDS might look at the state of a system, its stored information, whether in RAM, in the file-system, or elsewhere; and check that the contents of these appear as expected.

One can think of a HIDS as an agent that monitors whether anything/anyone - internal or external - has circumvented the security policy that the operating system tries to enforce. http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system

QUESTION 216
Which of the following usually provides reliable, real-time information without consuming network or host resources?

A. network-based IDS
B. host-based IDS
C. application-based IDS
D. firewall-based IDS

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
A network-based IDS usually provides reliable, real-time information without consuming network or host resources.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 217
The fact that a network-based IDS reviews packets payload and headers enable which of the following?

A. Detection of denial of service
B. Detection of all viruses
C. Detection of data corruption
D. Detection of all password guessing attacks

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Because a network-based IDS reviews packets and headers, denial of service attacks can also be detected.

This question is an easy question if you go through the process of elimination. When you see an answer containing the keyword: ALL It is something a give away that it is not the proper answer. On the real exam you may encounter a few question where the use of the work ALL renders the choice invalid. Pay close attention to such keyword.

The following are incorrect answers:

Even though most IDSs can detect some viruses and some password guessing attacks, they cannot detect ALL viruses or ALL password guessing attacks. Therefore these two answers are only detractors.
Unless the IDS knows the valid values for a certain dataset, it can NOT detect data corruption.

Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 218
Which of the following reviews system and event logs to detect attacks on the host and determine if the attack was successful?

A. host-based IDS

B. firewall-based IDS C. bastion-based IDS
D. server-based IDS

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
A host-based IDS can review the system and event logs in order to detect an attack on the host and to determine if the attack was successful.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 48.

QUESTION 219
What would be considered the biggest drawback of Host-based Intrusion Detection systems (HIDS)?

A. It can be very invasive to the host operating system
B. Monitors all processes and activities on the host system only
C. Virtually eliminates limits associated with encryption
D. They have an increased level of visibility and control compared to NIDS

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
The biggest drawback of HIDS, and the reason many organizations resist its use, is that it can be very invasive to the host operating system. HIDS must have the capability to monitor all processes and activities on the host system and this can sometimes interfere with normal system processing.

HIDS versus NIDS
A host-based IDS (HIDS) can be installed on individual workstations and/ or servers to watch for inappropriate or anomalous activity. HIDSs are usually used to make sure users do not delete system files, reconfigure important settings, or put the system at risk in any other way.

So, whereas the NIDS understands and monitors the network traffic, a HIDS's universe is limited to the computer itself. A HIDS does not understand or review network traffic, and a NIDS does not "look in" and monitor a system's activity. Each has its own job and stays out of the other's way.

The ISC2 official study book defines an IDS as:
An intrusion detection system (IDS) is a technology that alerts organizations to adverse or unwanted activity. An IDS can be implemented as part of a network device, such as a router, switch, or firewall, or it can be a dedicated IDS device monitoring traffic as it traverses the network. When used in this way, it is referred to as a network IDS, or NIDS. IDS can also be used on individual host systems to monitor and report on file, disk, and process activity on that host. When used in this way it is referred to as a host-based IDS, or HIDS.

An IDS is informative by nature and provides real-time information when suspicious activities are identified. It is primarily a detective device and, acting in this traditional role, is not used to directly prevent the suspected attack.

What about IPS?
In contrast, an intrusion prevention system (IPS), is a technology that monitors activity like an IDS but will automatically take proactive preventative action if it detects unacceptable activity. An IPS permits a predetermined set of functions and actions to occur on a network or system; anything that is not permitted is considered unwanted activity and blocked. IPS is engineered specifically to respond in real time to an event at the system or network layer. By proactively enforcing policy, IPS can thwart not only attackers, but also authorized users attempting to perform an action that is not within policy. Fundamentally, IPS is considered an access control and policy enforcement technology, whereas IDS is considered network monitoring and audit technology.

The following answers were incorrect:
All of the other answer were advantages and not drawback of using HIDS

TIP FOR THE EXAM:
Be familiar with the differences that exists between an HIDS, NIDS, and IPS. Know that IDS's are mostly detective but IPS are preventive. IPS's are considered an access control and policy enforcement technology, whereas IDS's are considered network monitoring and audit technology.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5817-5822). McGraw-Hill. Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Access Control ((ISC)2 Press), Domain1, Page 180-188 or on the kindle version look for Kindle Locations 3199-3203. Auerbach Publications.

QUESTION 220
Attributes that characterize an attack are stored for reference using which of the following Intrusion Detection System (IDS) ?

A. signature-based IDS
B. statistical anomaly-based IDS
C. event-based IDS
D. inferent-based IDS

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 221

Which of the following is an issue with signature-based intrusion detection systems?

A. Only previously identified attack signatures are detected.
B. Signature databases must be augmented with inferential elements.
C. It runs only on the windows operating systemD. Hackers can circumvent signature evaluations.

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
An issue with signature-based ID is that only attack signatures that are stored in their database are detected.

New attacks without a signature would not be reported. They do require constant updates in order to maintain their effectiveness.

Reference used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 222
Which of the following is an IDS that acquires data and defines a "normal" usage profile for the network or host?

A. Statistical Anomaly-Based ID B.
Signature-Based ID
C. dynamical anomaly-based ID

D. inferential anomaly-based ID

Correct Answer: A
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Statistical Anomaly-Based ID - With this method, an IDS acquires data and defines a "normal" usage profile for the network or host that is being monitored.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 223
Which of the following is a disadvantage of a statistical anomaly-based intrusion detection system?

A. it may truly detect a non-attack event that had caused a momentary anomaly in the system.

B. it may falsely detect a non-attack event that had caused a momentary anomaly in the system.
C. it may correctly detect a non-attack event that had caused a momentary anomaly in the system.
D. it may loosely detect a non-attack event that had caused a momentary anomaly in the system.

Correct Answer: B
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Some disadvantages of a statistical anomaly-based ID are that it will not detect an attack that does not significantly change the system operating characteristics, or it may falsely detect a non-attack event that had caused a momentary anomaly in the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

QUESTION 224
In the process of gathering evidence from a computer attack, a system administrator took a series of actions which are listed below. Can you identify which one of these actions has compromised the whole evidence collection process?

A. Using a write blocker
B. Made a full-disk image
C. Created a message digest for log files
D. Displayed the contents of a folder

Correct Answer: D
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Displaying the directory contents of a folder can alter the last access time on each listed file.

Using a write blocker is wrong because using a write blocker ensure that you cannot modify the data on the host and it prevent the host from writing to its hard drives.

Made a full-disk image is wrong because making a full-disk image can preserve all data on a hard disk, including deleted files and file fragments.

Created a message digest for log files is wrong because creating a message digest for log files. A message digest is a cryptographic checksum that can demonstrate that the integrity of a file has not been compromised (e.g. changes to the content of a log file)

Domain: LEGAL, REGULATIONS, COMPLIANCE AND INVESTIGATIONS

References:
AIO 3rd Edition, page 783-784
NIST 800-61 Computer Security Incident Handling guide page 3-18 to 3-20

QUESTION 225
As a result of a risk assessment, your security manager has determined that your organization needs to implement an intrusion detection system that can detect unknown attacks and can watch for unusual traffic behavior, such as a new service appearing on the network. What type of intrusion detection system would you select?

A. Protocol anomaly based
B. Pattern matching
C. Stateful matching
D. Traffic anomaly-based

Correct Answer: D
Section: Analysis and Monitoring
Explanation

Explanation/Reference:
Traffic anomaly-based is the correct choice. An anomaly based IDS can detect unknown attacks. A traffic anomaly based IDS identifies any unacceptable deviation from expected behavior based on network traffic.

Protocol anomaly based is not the best choice as while a protocol anomaly based IDS can identify unknown attacks, this type of system is more suited to identifying deviations from established protocol standards such as HTTP. This type of IDS faces problems in analyzing complex or custom protocols.

Pattern matching is not the best choice as a pattern matching IDS cannot identify unknown attacks. This type of system can only compare packets against signatures of known attacks.

Stateful matching is not the best choice as a statful matching IDS cannot identify unknown attacks. This type of system works by scanning traffic streams for patterns or signatures of attacks.

Reference:
Official guide to the CISSP CBK. pages 198 to 201

QUESTION 226
Which of the following recovery plan test results would be most useful to management?

A. elapsed time to perform various activities.
B. list of successful and unsuccessful activities.
C. amount of work completed.
D. description of each activity.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
After a test has been performed the most useful test results for manangement would be knowing what worked and what didn't so that they could correct the mistakes where needed.

The following answers are incorrect:

elapsed time to perform various activities. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

amount of work completed. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

description of each activity. This is incorrect because it is not the best answer, these results are not as useful as list of successful and unsuccessful activities would be to managment.

QUESTION 227
Which of the following computer recovery sites is only partially equipped with processing equipment?

A. hot site
B. rolling hot site
C. warm site
D. cold site

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A warm site has some basic equipment or in some case almost all of the equipment but it is not sufficient to be operational without bringing in the last backup and in some cases more computers and other equipment.

The following answers are incorrect:

hot site. Is incorrect because a hot-site is fully configured with all the required hardware. The only thing missing is the last backup and you are up and running.

Rolling hot site. Is incorrect because a rolling hot-site is fully configured with all the required hardware.

cold site. Is incorrect because a cold site has basically power, HVAC, basic cabling, but no or little as far as processing equipment is concerned. All other equipment must be brought to this site. It might take a week or two to reconstruct.

References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

QUESTION 228
Which of the following computer recovery sites is the least expensive and the most difficult to test?

A. non-mobile hot site
B. mobile hot site
C. warm site
D. cold site

Correct Answer: D
Section: Risk, Response and Recovery

Explanation

Explanation/Reference:
Is the least expensive because it is basically a structure with power and would be the most difficult to test because you would have to install all of the hardware infrastructure in order for it to be operational for the test.

The following answers are incorrect:

non-mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.

mobile hot site. Is incorrect because it is more expensive then a cold site and easier to test because all of the infrastructure is in place.

warm site. Is incorrect because it is more expensive then a cold site and easier to test because more of the infrastructure is in place.

QUESTION 229
Which of the following is the most important consideration in locating an alternate computing facility during the development of a disaster recovery plan?

A. It is unlikely to be affected by the same disaster.
B. It is close enough to become operational quickly.
C. It is close enough to serve its users.
D. It is convenient to airports and hotels.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.

From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.

The following answers are incorrect:

It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.

It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well

It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.

References:

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)
NIST document 800-34 pg 21

QUESTION 230
Contracts and agreements are often times unenforceable or hard to enforce in which of the following alternate facility recovery agreement?

A. hot site
B. warm site
C. cold site
D. reciprocal agreement

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A reciprocal agreement is where two or more organizations mutually agree to provide facilities to the other if a disaster occurs. The organizations must have similiar hardware and software configurations. Reciprocal agreements are often not legally binding.

Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you.

Government regulators do not accept reciprocal agreements as valid disaster recovery sites.

Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.

Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.

With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.

References:
OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

The following answers are incorrect:
hot site. Is incorrect because you have a contract in place stating what services are to be provided.
warm site. Is incorrect because you have a contract in place stating what services are to be provided.
cold site. Is incorrect because you have a contract in place stating what services are to be provided.

QUESTION 231
Organizations should not view disaster recovery as which of the following?

A. Committed expense.
B. Discretionary expense.
C. Enforcement of legal statutes.
D. Compliance with regulations.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Disaster Recovery should never be considered a discretionary expense. It is far too important a task. In order to maintain the continuity of the business Disaster Recovery should be a commitment of and by the organization.

A discretionary fixed cost has a short future planning horizon—under a year. These types of costs arise from annual decisions of management to spend in specific fixed cost areas, such as marketing and research. DR would be an ongoing long term committment not a short term effort only.

A committed fixed cost has a long future planning horizon— more than on year. These types of costs relate to a company's investment in assets such as facilities and equipment. Once such costs have been incurred, the company is required to make future payments.

The following answers are incorrect:

committed expense. Is incorrect because Disaster Recovery should be a committed expense.

enforcement of legal statutes. Is incorrect because Disaster Recovery can include enforcement of legal statutes. Many organizations have legal requirements toward Disaster Recovery.

compliance with regulations. Is incorrect because Disaster Recovery often means compliance with regulations. Many financial institutions have regulations requiring Disaster Recovery Plans and Procedures.

QUESTION 232
Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
There are some conflicting figures as to which group is a bigger threat hackers or employees. Employees are still considered to the leading source of computer crime losses. Employees often have an easier time gaining access to systems or source code then ousiders or other means of creating computer crimes.

A word of caution is necessary: although the media has tended to portray the threat of cybercrime as existing almost exclusively from the outside, external to a company, reality paints a much different picture. Often the greatest risk of cybercrime comes from the inside, namely, criminal insiders. Information security professionals must be particularly sensitive to the phenomena of the criminal or dangerous insider, as these individuals usually operate under the radar, inside of the primarily outward/external facing security controls, thus significantly increasing the impact of their crimes while leaving few, if any, audit trails to follow and evidence for prosecution.

Some of the large scale crimes committed agains bank lately has shown that Internal Threats are the worst and they are more common that one would think. The definition of what a hacker is can vary greatly from one country to another but in some of the states in the USA a hacker is defined as Someone who is using resources in a way that is not authorized. A recent case in Ohio involved an internal employee who was spending most of his day on dating website looking for the love of his life. The employee was taken to court for hacking the company resources.

The following answers are incorrect:

hackers. Is incorrect because while hackers represent a very large problem and both the frequency of attacks and overall losses have grown hackers are considered to be a small segment of combined computer fraudsters.

industrial saboteurs. Is incorrect because industrial saboteurs tend to go after trade secrets. While the loss to the organization can be great, they still fall short when compared to the losses created by employees. Often it is an employee that was involved in industrial sabotage.

foreign intelligence officers. Is incorrect because the losses tend to be national secrets. You really can't put t cost on this and the number of frequency and occurances of this is less than that of employee related losses.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 22327-22331). Auerbach Publications. Kindle Edition.

QUESTION 233
Which of the following is the best reason for the use of an automated risk analysis tool?

A. Much of the data gathered during the review cannot be reused for subsequent analysis.
B. Automated methodologies require minimal training and knowledge of risk analysis.
C. Most software tools have user interfaces that are easy to use and does not require any training.
D. Information gathering would be minimized and expedited due to the amount of information already built into the tool.

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The use of tools simplifies this process. Not only do they usually have a database of assests, threats, and vulnerabilities but they also speed up the entire process.

Using Automated tools for performing a risk assessment can reduce the time it takes to perform them and can simplify the process as well. The better types of these tools include a well-researched threat population and associated statistics. Using one of these tools virtually ensures that no relevant threat is overlooked, and associated risks are accepted as a consequence of the threat being overlooked.

In most situations, the assessor will turn to the use of a variety of automated tools to assist in the vulnerability assessment process. These tools contain extensive databases of specific known vulnerabilities as well as the ability to analyze system and network configuration information to predict where a particular system might be vulnerable to different types of attacks. There are many different types of tools currently available to address a wide variety of vulnerability assessment needs. Some tools will examine a system from the viewpoint of the network, seeking to determine if a system can be compromised by a remote attacker exploiting available services on a particular host system. These tools will test for open ports listening for connections, known vulnerabilities in common services, and known operating system exploits.

Michael Gregg says:
Automated tools are available that minimize the effort of the manual process. These programs enable users to rerun the analysis with different parameters to answer "what-ifs." They perform calculations quickly and can be used to estimate future expected losses easier than performing the calculations manually.

Shon Harris in her latest book says:
The gathered data can be reused, greatly reducing the time required to perform subsequent analyses. The risk analysis team can also print reports and comprehensive graphs to present to management.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 4655-4661). Auerbach Publications. Kindle Edition.

and

CISSP Exam Cram 2 by Michael Gregg
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 2333-2335). McGraw-Hill. Kindle Edition.

The following answers are incorrect:

Much of the data gathered during the review cannot be reused for subsequent analysis. Is incorrect because the data can be reused for later analysis.

Automated methodologies require minimal training and knowledge of risk analysis. Is incorrect because it is not the best answer. While a minimal amount of training and knowledge is needed, the analysis should still be performed by skilled professionals.

Most software tools have user interfaces that are easy to use and does not require any training. Is incorrect because it is not the best answer. While many of the user interfaces are easy to use it is better if the tool already has information built into it. There is always a training curve when any product is being used for the first time.

QUESTION 234
A deviation from an organization-wide security policy requires which of the following?

A. Risk Acceptance
B. Risk Assignment
C. Risk Reduction
D. Risk Containment

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A deviation from an organization-wide security policy requires you to manage the risk. If you deviate from the security policy then you are required to accept the risks that might occur.

In some cases, it may be prudent for an organization to simply accept the risk that is presented in certain scenarios. Risk acceptance is the practice of accepting certain risk(s), typically based on a business decision that may also weigh the cost versus the benefit of dealing with the risk in another way.

The OIG defines Risk Management as: This term characterizes the overall process.

The first phase of risk assessment includes identifying risks, risk-reducing measures, and the budgetary impact of implementing decisions related to the acceptance, avoidance, or transfer of risk.

The second phase of risk management includes the process of assigning priority to, budgeting, implementing, and maintaining appropriate risk-reducing measures.

Risk management is a continuous process of ever-increasing complexity. It is how we evaluate the impact of exposures and respond to them. Risk management minimizes loss to information assets due to undesirable events through identification, measurement, and control. It encompasses the overall security review, risk analysis, selection and evaluation of safeguards, cost–benefit analysis, management decision, and safeguard identification and implementation, along with ongoing effectiveness review.

Risk management provides a mechanism to the organization to ensure that executive management knows current risks, and informed decisions can be made to use one of the risk management principles: risk avoidance, risk transfer, risk mitigation, or risk acceptance. The 4 ways of dealing with risks are: Avoidance, Transfer, Mitigation, Acceptance

The following answers are incorrect:

Risk assignment. Is incorrect because it is a distractor, assignment is not one of the ways to manage risk.

Risk reduction. Is incorrect because there was a deviation of the security policy. You could have some additional exposure by the fact that you deviated from the policy.

Risk containment. Is incorrect because it is a distractor, containment is not one of the ways to manage risk.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 8882-8886). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10206-10208). Auerbach Publications. Kindle Edition.

QUESTION 235
Which of the following is biggest factor that makes Computer Crimes possible?

A. The fraudster obtaining advanced training & special knowledge.
B. Victim carelessness.
C. Collusion with others in information processing.
D. System design flaws.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The biggest factor that makes Computer Crimes possible is Victim Carelessness. Awareness and education can reduce the chance of someone becomming a victim.

The types and frequency of Computer Crimes are increasing at a rapid rate. Computer Crime was once mainly the result of insiders or disgruntled employees. Now just about everybody has access to the internet, professional criminals are taking advantage of this.

Specialized skills are no longer needed and a search on the internet can provide a fraudster with a plethora of tools that can be used to perpetuate fraud.

All too often carelessness leads to someone being a victim. People often use simple passwords or write them down in plain sight where they can be found by fraudsters. People throwing away papers loaded with account numbers, social security numbers, or other types of non-public personal information. There are phishing e-mail attempts where the fraudster tries to redirect a potential victim to a bogus site that resembles a legitimate site in an attempt to get the users' login ID and password, or other credentials. There is also social engineering. Awareness and training can help reduce the chance of someone becoming a victim.

The following answers are incorrect:

The fraudster obtaining advanced training and special knowledge. Is incorrect because training and special knowledge is not required. There are many tools widely available to fraudsters.

Collusion with others in information processing. Is incorrect because as more and more people use computers in their daily lives, it is no longer necessary to have someone on the inside be a party to fraud attempts.

System design flaws. Is incorrect because while System design flaws are sometimes a factor in Computer Crimes more often then not it is victim carelessness that leads to Computer Crimes.

References:
OIG CBK Legal, Regulations, Compliance and Investigations (pages 695 - 697)

QUESTION 236
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?

A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.
D. If the defense has no objections.

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.

The following answers are incorrect:

When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.

When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.

If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

QUESTION 237
In addition to the Legal Department, with what company function must the collection of physical evidence be coordinated if an employee is suspected?

A. Human Resources
B. Industrial Security
C. Public Relations
D. External Audit Group

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
If an employee is suspected of causing an incident, the human resources department may be involved—for example, in assisting with disciplinary proceedings.

Legal Department. The legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. In addition, the guidance of the general counsel or legal department should be sought if there is reason to believe that an incident may have legal ramifications, including evidence collection, prosecution of a suspect, or a lawsuit, or if there may be a need for a memorandum of understanding (MOU) or other binding agreements involving liability limitations for information sharing.

Public Affairs, Public Relations, and Media Relations. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public.

The Incident response team members could include:

Management

Information Security
Legal / Human Resources
Public Relations
Communications
Physical Security
Network Security
Network and System Administrators
Network and System Security Administrators
Internal Audit

Events versus Incidents
An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt. Adverse events are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data. This guide addresses only adverse events that are computer security- related, not those caused by natural disasters, power failures, etc.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Examples of incidents are:
An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.

Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.

An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

A user provides or exposes sensitive information to others through peer-to-peer file sharing services.

The following answers are incorrect:

Industrial Security. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.

public relations. Is incorrect because it is not the best answer. It would be an important element to minimize public image damage but not the best choice for this question.

External Audit Group. Is incorrect because it is not the best answer, the human resource department must be involved with the collection of physical evidence if an employee is suspected.

Reference(s) used for this question:
NIST Special Publication 800-61

QUESTION 238
To be admissible in court, computer evidence must be which of the following?

A. Relevant
B. Decrypted
C. Edited
D. Incriminating

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Before any evidence can be admissible in court, the evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. This holds true for computer evidence as well.

While there are no absolute means to ensure that evidence will be allowed and helpful in a court of law, information security professionals should understand the basic rules of evidence. Evidence should be relevant, authentic, accurate, complete, and convincing. Evidence gathering should emphasize these criteria.

As stated in CISSP for Dummies:

Because computer-generated evidence can sometimes be easily manipulated, altered , or tampered with, and because it's not easily and commonly understood, this type of evidence is usually considered suspect in a court of law. In order to be admissible, evidence must be

Relevant: It must tend to prove or disprove facts that are relevant and material to the case.

Reliable: It must be reasonably proven that what is presented as evidence is what was originally collected and that the evidence itself is reliable. This is accomplished, in part, through proper evidence handling and the chain of custody. (We discuss this in the upcoming section "Chain of custody and the evidence life cycle.")

Legally permissible: It must be obtained through legal means. Evidence that's not legally permissible may include evidence obtained through the following means:

Illegal search and seizure: Law enforcement personnel must obtain a prior court order; however, non-law enforcement personnel, such as a supervisor or system administrator, may be able to conduct an authorized search under some circumstances.

Illegal wiretaps or phone taps: Anyone conducting wiretaps or phone taps must obtain a prior court order.

Entrapment or enticement: Entrapment encourages someone to commit a crime that the individual may have had no intention of committing. Conversely, enticement lures someone toward certain evidence (a honey pot, if you will) after that individual has already committed a crime. Enticement is not necessarily illegal but does raise certain ethical arguments and may not be admissible in court.

Coercion: Coerced testimony or confessions are not legally permissible.

Unauthorized or improper monitoring: Active monitoring must be properly authorized and conducted in a standard manner; users must be notified that they may be subject to monitoring. The following answers are incorrect:

decrypted. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.

edited. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence. Edited evidence violates the rules of evidence.

incriminating. Is incorrect because evidence has to be relevant, material to the issue, and it must be presented in compliance with the rules of evidence.

Reference(s) used for this question:

CISSP STudy Guide (Conrad, Misenar, Feldman) Elsevier. 2012. Page 423

and
Mc Graw Hill, Shon Harris CISSP All In One (AIO), 6th Edition , Pages 1051-1056
and
CISSP for Dummies , Peter Gregory

QUESTION 239
The typical computer fraudsters are usually persons with which of the following characteristics?

A. They have had previous contact with law enforcement
B. They conspire with others
C. They hold a position of trust
D. They deviate from the accepted norms of society

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
These people, as employees, are trusted to perform their duties honestly and not take advantage of the trust placed in them.

The following answers are incorrect:

They have had previous contact with law enforcement. Is incorrect because most often it is a person that holds a position of trust and this answer implies they have a criminal background. This type of individual is typically not in a position of trust within an organization.

They conspire with others. Is incorrect because they typically work alone, often as a form of retribution over a percieved injustice done to them.

They deviate from the accepted norms of society. Is incorrect because while the nature of fraudsters deviate from the norm, the fraudsters often hold a position of trust within the organization.

QUESTION 240
Once evidence is seized, a law enforcement officer should emphasize which of the following?

A. Chain of command
B. Chain of custody
C. Chain of control
D. Chain of communications

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
All people that handle the evidence from the time the crime was committed through the final disposition must be identified. This is to ensure that the evidence can be used and has not been tampered with.

The following answers are incorrect:

chain of command. Is incorrect because chain of command is the order of authority and does not apply to evidence.

chain of control. Is incorrect because it is a distractor. chain of
communications. Is incorrect because it is a distractor.

QUESTION 241
Which of the following cannot be undertaken in conjunction or while computer incident handling is ongoing?

A. System development activity
B. Help-desk function
C. System Imaging
D. Risk management process

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
If Incident Handling is underway an incident has potentially been identified. At that point all use of the system should stop because the system can no longer be trusted and any changes could contaminate the evidence. This would include all System Development Activity.

Every organization should have plans and procedures in place that deals with Incident Handling.

Employees should be instructed what steps are to be taken as soon as an incident occurs and how to report it. It is important that all parties involved are aware of these steps to protect not only any possible evidence but also to prevent any additional harm.

It is quite possible that the fraudster has planted malicous code that could cause destruction or even a Trojan Horse with a back door into the system. As soon as an incident has been identified the system can no longer be trusted and all use of the system should cease.

Shon Harris in her latest book mentions:
Although we commonly use the terms “event” and “incident” interchangeably, there are subtle differences between the two. An event is a negative occurrence that can be observed, verified, and documented, whereas an incident is a series of events that negatively affects the company and/ or impacts its security posture. This is why we call reacting to these issues “incident response” (or “incident handling”), because something is negatively affecting the company and causing a security breach.

Many types of incidents (virus, insider attack, terrorist attacks, and so on) exist, and sometimes it is just human error. Indeed, many incident response individuals have received a frantic call in the middle of the night because a system is acting “weird.” The reasons could be that a deployed patch broke something, someone misconfigured a device, or the administrator just learned a new scripting language and rolled out some code that caused mayhem and confusion.

When a company endures a computer crime, it should leave the environment and evidence unaltered and contact whomever has been delegated to investigate these types of situations. Someone who is unfamiliar with the proper process of collecting data and evidence from a crime scene could instead destroy that evidence, and thus all hope of prosecuting individuals, and achieving a conviction would be lost.

Companies should have procedures for many issues in computer security such as enforcement procedures, disaster recovery and continuity procedures, and backup procedures. It is also necessary to have a procedure for dealing with computer incidents because they have become an increasingly important issue of today’s information security departments. This is a direct result of attacks against networks and information systems increasing annually. Even though we don’t have specific numbers due to a lack of universal reporting and reporting in general, it is clear that the volume of attacks is increasing.

Just think about all the spam, phishing scams, malware, distributed denial-of-service, and other attacks you see on your own network and hear about in the news. Unfortunately, many companies are at a loss as to who to call or what to do right after they have been the victim of a cybercrime. Therefore, all companies should have an incident response policy that indicates who has the authority to initiate an incident response, with supporting procedures set up before an incident takes place.

This policy should be managed by the legal department and security department. They need to work together to make sure the technical security issues are covered and the legal issues that surround criminal activities are properly dealt with. The incident response policy should be clear and concise. For example, it should indicate if systems can be taken offline to try to save evidence or if systems have to continue functioning at the risk of destroying evidence. Each system and functionality should have a priority assigned to it. For instance, if the file server is infected, it should be removed from the network, but not shut down. However, if the mail server is infected, it should not be removed from the network or shut down because of the priority the company attributes to the mail server over the file server. Tradeoffs and decisions will have to be made, but it is better to think through these issues before the situation occurs, because better logic is usually possible before a crisis, when there's less emotion and chaos.

The Australian Computer Emergency Response Team's General Guidelines for Computer Forensics:

Keep the handling and corruption of original data to a minimum.
Document all actions and explain changes.
Follow the Five Rules for Evidence (Admissible, Authentic, Complete, Accurate, Convincing).
• Bring in more experienced help when handling and/ or analyzing the evidence is beyond your knowledge, skills, or abilities.
Adhere to your organization's security policy and obtain written permission to conduct a forensics
investigation. Capture as accurate an image of the system(s) as possible while working quickly. Be ready to
testify in a court of law.
Make certain your actions are repeatable.
Prioritize your actions, beginning with volatile and proceeding to persistent evidence.
Do not run any programs on the system(s) that are potential evidence.
Act ethically and in good faith while conducting a forensics investigation, and do not attempt to do any harm.

The following answers are incorrect:

help-desk function. Is incorrect because during an incident, employees need to be able to communicate with a central source. It is most likely that would be the help-desk. Also the help-desk would need to be able to communicate with the employees to keep them informed.

system imaging. Is incorrect because once an incident has occured you should perform a capture of evidence starting with the most volatile data and imaging would be doen using bit for bit copy of storage medias to protect the evidence.

risk management process. Is incorrect because incident handling is part of risk management, and should continue.

Reference(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21468-21476). McGraw-Hill. Kindle Edition.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 21096-21121). McGraw-Hill. Kindle Edition.
and

NIST Computer Security incident handling http://csrc.nist.gov/publications/nistpubs/800-12/800-12-html/chapter12.html

QUESTION 242
Devices that supply power when the commercial utility power system fails are called which of the following?

A. power conditioners
B. uninterruptible power supplies

C. power filters
D. power dividers

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
From Shon Harris AIO Fifth Edition:

Protecting power can be done in three ways: through UPSs, power line conditioners, and backup sources.

UPSs use battery packs that range in size and capacity. A UPS can be online or standby.

Online UPS systems use AC line voltage to charge a bank of batteries. When in use, the UPS has an inverter that changes the DC output from the batteries into the required AC form and that regulates the voltage as it powers computer devices.

Online UPS systems have the normal primary power passing through them day in and day out. They constantly provide power from their own inverters, even when the electric power is in proper use. Since the environment's electricity passes through this type of UPS all the time, the UPS device is able to quickly detect when a power failure takes place. An online UPS can provide the necessary electricity and picks up the load after a power failure much more quickly than a standby UPS.

Standby UPS devices stay inactive until a power line fails. The system has sensors that detect a power failure, and the load is switched to the battery pack. The switch to the battery pack is what causes the small delay in electricity being provided.
So an online UPS picks up the load much more quickly than a standby UPS, but costs more of course.

QUESTION 243

Within the realm of IT security, which of the following combinations best defines risk?

A. Threat coupled with a breach
B. Threat coupled with a vulnerability
C. Vulnerability coupled with an attack
D. Threat coupled with a breach of security

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Answer: Threat coupled with a vulnerability. Threats are circumstances or actions with the ability to harm a system. They can destroy or modify data or result an a DoS. Threats by themselves are not acted upon unless there is a vulnerability that can be taken advantage of. Risk enters the equation when a vulnerability (Flaw or weakness) exists in policies, procedures, personnel management, hardware, software or facilities and can be exploited by a threat agent. Vulnerabilities do not cause harm, but they leave the system open to harm. The combination of a threat with a vulnerability increases the risk to the system of an intrusion.

The following answers are incorrect:

Threat coupled with a breach. A threat is the potential that a particular threat-source will take advantage of a vulnerability. Breaches get around security. It does not matter if a breach is discovered or not, it has still occured and is not a risk of something occuring. A breach would quite often be termed as an incident or intrusion.

Vulnerability coupled with an attack. Vulnerabilities are weaknesses (flaws) in policies, procedures, personnel management, hardware, software or factilities that may result in a harmful intrusion to an IT system. An attack takes advantage of the flaw or vulnerability. Attacks are explicit attempts to violate security, and are more than risk as they are active.

Threat coupled with a breach of security. This is a detractor. Although a threat agent may take advantage of (Breach) vulnerabilities or flaws in systems security. A threat coupled with a breach of security is more than a risk as this is active.

The following reference(s) may be used to research the Qs in this question:

ISC2 OIG, 2007 p. 66-67
Shon Harris AIO v3 p. 71-72

QUESTION 244
Which of the following backup sites is the most effective for disaster recovery?

A. Time brokers
B. Hot sites
C. Cold sites
D. Reciprocal Agreement

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A hot site has the equipment, software and communications capabilities to facilitate a recovery within a few minutes or hours following the notification of a disaster to the organization's primary site. With the exception of providing your own hot site, commercial hot sites provide the greatest protection. Most will allow you up to six weeks to restore your sites if you declare a disaster. They also permit an annual amount of time to test the Disaster Plan.

The following answers are incorrect:

Cold sites. Cold sites are empty computer rooms consisting only of environmental systems, such as air conditioning and raised floors, etc. They do not meet the requirements of most regulators and boards of directors that the disaster plan be tested at least annually.

Reciprocal Agreement. Reciprocal agreements are not contracts and cannot be enforced. You cannot force someone you have such an agreement with to provide processing to you. Government regulators do not accept reciprocal agreements as valid disaster recovery backup sites.

Time Brokers. Time Brokers promise to deliver processing time on other systems. They charge a fee, but cannot guaranty that processing will always be available, especially in areas that experienced multiple disasters.

The following reference(s) were/was used to create this question:

ISC2 OIG, 2007 p368
Shon Harris AIO v3. p.710

QUESTION 245
Which of the following is NOT a transaction redundancy implementation?

A. on-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing

Correct Answer: A
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
Three concepts are used to create a level of fault tolerance and redundancy in transaction processing.

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

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

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

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

Reference used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407). Auerbach Publications. Kindle Edition. and
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20375-20377). Auerbach Publications. Kindle Edition.

QUESTION 246

Which of the following steps is NOT one of the eight detailed steps of a Business Impact Assessment (BIA):

A. Notifying senior management of the start of the assessment.
B. Creating data gathering techniques.
C. Identifying critical business functions.
D. Calculating the risk for each different business function.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Source: HARRIS, S., CISSP All- In-One Exam Guide, 3rd. Edition, 2005, Chapter 9, Page 701.

There have been much discussion about the steps of the BIA and I struggled with this before deciding to scrape the question about "the four steps," and re-write the question using the AIO for a reference. This question should be easy.... if you know all eight steps.

The eight detailed and granular steps of the BIA are:

1. Select Individuals to interview for the data gathering.
2. Create data gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources that these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and the threats to these functions.
7. Calculate risk for each of the different business functions.
8. Document findings and report them to management.

Shon goes on to cover each step in Chapter 9.

QUESTION 247
Which of the following results in the most devastating business interruptions?

A. Loss of Hardware/Software
B. Loss of Data
C. Loss of Communication Links
D. Loss of Applications

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Source: Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.
All of the others can be replaced or repaired. Data that is lost and was not backed up, cannot be restored.

QUESTION 248
Which of the following is the most critical item from a disaster recovery point of view?

A. Data
B. Hardware/Software
C. Communication LinksD. Software Applications

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The most important point is ALWAYS the data. Everything else can be replaced or repaired.

Data MUST be backed up, backups must be regularly tested, because once it is truly lost, it is lost forever.

The goal of disaster recovery is to minimize the effects of a disaster or disruption. It means taking the necessary steps to ensure that the resources, personnel, and business processes are able to resume operation in a timely manner . This is different from continuity planning, which provides methods and procedures for dealing with longer-term outages and disasters.

The goal of a disaster recovery plan is to handle the disaster and its ramifications right after the disaster hits; the disaster recovery plan is usually very information technology (IT)– focused. A disaster recovery plan (DRP) is carried out when everything is still in emergency mode, and everyone is scrambling to get all critical systems back online.

Reference(s) used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 887). McGraw-Hill. Kindle Edition.
and
Veritas eLearning CD - Introducing Disaster Recovery Planning, Chapter 1.

QUESTION 249

Which of the following is defined as the most recent point in time to which data must be synchronized without adversely affecting the organization (financial or operational impacts)?

A. Recovery Point Objective
B. Recovery Time Objective
C. Point of Time Objective
D. Critical Time Objective

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The recovery point objective (RPO) is the maximum acceptable level of data loss following an unplanned “event”, like a disaster (natural or man-made), act of crime or terrorism, or any other business or technical disruption that could cause such data loss. The RPO represents the point in time, prior to such an event or incident, to which lost data can be recovered (given the most recent backup copy of the data).

The recovery time objective (RTO) is a period of time within which business and / or technology capabilities must be restored following an unplanned event or disaster. The RTO is a function of the extent to which the interruption disrupts normal operations and the amount of revenue lost per unit of time as a result of the disaster.

These factors in turn depend on the affected equipment and application(s). Both of these numbers represent key targets that are set by key businesses during business continuity and disaster recovery planning; these targets in turn drive the technology and implementation choices for business resumption services, backup / recovery / archival services, and recovery facilities and procedures.

Many organizations put the cart before the horse in selecting and deploying technologies before understanding the business needs as expressed in RPO and RTO; IT departments later bear the brunt of user complaints that their service expectations are not being met. Defining the RPO and RTO can avoid that pitfall, and in doing so can also make for a compelling business case for recovery technology spending and staffing.

For the CISSP candidate studying for the exam, there are no such objectives for "point of time," and "critical time." Those two answers are simply detracters.

Reference:
http://www.wikibon.org/Recovery_point_objective_/_recovery_time_objective_strategy

QUESTION 250
Valuable paper insurance coverage does not cover damage to which of the following?

A. Inscribed, printed and Written documents
B. Manuscripts

C. Records
D. Money and Securities

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.

Stop and ask yourself what happens if your business lost those documents today.

Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records. Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data,programs or instructions used in your data processing operations, including the materials on which the data is recorded."

The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to $25,000.

It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.

The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.

For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher. Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?

Often when a business owner considers the actual cost related to the reproduction of records, the owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.
Insurers (and your insurance professional)will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.

Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

Reference(s) used for this question:
http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm

QUESTION 251
Which of the following is covered under Crime Insurance Policy Coverage?

A. Inscribed, printed and Written documents
B. Manuscripts
C. Accounts Receivable
D. Money and Securities

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Property Insurance overview, Page 589.

QUESTION 252
If your property Insurance has Actual Cash Valuation (ACV) clause, your damaged property will be compensated based on:

A. Value of item on the date of loss
B. Replacement with a new item for the old one regardless of condition of lost item
C. Value of item one month before the loss
D. Value of item on the date of loss plus 10 percent

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
This is called the Actual Cash Value (ACV) or Actual Cost Valuation (ACV)

All of the other answers were only detractors. Below you have an explanation of the different types of valuation you could use. It is VERY important for you to validate with your insurer which one applies to you as you could have some very surprising finding the day you have a disaster that takes place.

Replacement Cost
Property replacement cost insurance promises to replace old with new. Generally, replacement of a building must be done on the same premises and used for the same purpose, using materials comparable to the quality of the materials in the damaged or destroyed property.

There are some other limitations to this promise. For example, the cost of repairs or replacement for buildings doesn't include the increased cost associated with building codes or other laws controlling how buildings must be built today. An endorsement adding coverage for the operation of Building Codes and the increased costs associated with complying with them is available separately — usually for additional premium. In addition, some insurance underwriters will only cover certain property on a depreciated value (actual cash value — ACV) basis even when attached to the building. This includes awnings and floor coverings, appliances for refrigerating, ventilating, cooking, dishwashing, and laundering. Depreciated value also applies to outdoor equipment or furniture.

Actual Cash Value (ACV)
The ACV is the default valuation clause for commercial property insurance. It is also known as depreciated value, but this is not the same as accounting depreciated value. The actual cash value is determined by first calculating the replacement value of the property. The next step involves estimating the amount to be subtracted, which reflects the building's age, wear, and tear.

This amount deducted from the replacement value is known as depreciation. The amount of depreciation is reduced by inflation (increased cost of replacing the property); regular maintenance; and repair (new roofs, new electrical systems, etc.) because these factors reduce the effective age of the buildings.

The amount of depreciation applicable is somewhat subjective and certainly subject to negotiation. In fact, there is often disagreement and a degree of uncertainty over the amount of depreciation applicable to a particular building.

Given this reality, property owners should not leave the determination of depreciation to chance or wait until suffering

a property loss to be concerned about it. Every three to five years, property owners should obtain a professional appraisal of the replacement value and depreciated value of the buildings.

The ACV valuation is an option for directors to consider when certain buildings are in need of repair, or budget constraints prevent insuring all of your facilities on a replacement cost basis. There are other valuation options for property owners to consider as well.

Functional Replacement Cost
This valuation method has been available for some time but has not been widely used. It is beginning to show up on property insurance policies imposed by underwriters with concerns about older, buildings. It can also be used for buildings, which are functionally obsolete.

This method provides for the replacement of a building with similar property that performs the same function, using less costly material. The endorsement includes coverage for building codes automatically.

In the event of a loss, the insurance company pays the smallest of four payment options.

1. In the event of a total loss, the insurer could pay the limit of insurance on the building or the cost to replace the building on the same (or different) site with a payment that is “functionally equivalent.”

2. In the event of a partial loss, the insurance company could pay the cost to repair or replace the damaged portion in the same architectural style with less costly material (if available).

3. The insurance company could also pay the amount actually spent to demolish the undamaged portion of the building and clear the site if necessary.

4. The fourth payment option is to pay the amount actually spent to repair, or replace the building using less costly materials, if available (Hillman and McCracken 1997).

Unlike the replacement cost valuation method, which excluded certain fixtures and personal property used to service the premises, this endorsement provides functional replacement cost coverage for these items (awnings, floor coverings, appliances, etc.) (Hillman nd McCracken 1997).

As in the standard replacement cost value option, the insured can elect not to repair or replace the property. Under these circumstances the company pays the smallest of the following:

1. The Limit of Liability

2. The “market value” (not including the value of the land) at the time of the loss. The endorsement defines “market value” as the price which the property might be expected to realize if ffered for sale in fair market.”

3. A modified form of ACV (the amount to repair or replace on he same site with less costly material and in the same architectural tyle, less depreciation) (Hillman and McCracken 1997).

Agreed Value or Agreed Amount
Agreed value or agreed amount is not a valuation method. Instead, his term refers to a waiver of the coinsurance clause in the property insurance policy. Availability of this coverage feature varies among insurers but, it is usually available only when the underwriter has proof (an independent appraisal, or compliance with an insurance company valuation model) of the value of your property. When do I get paid?

Generally, the insurance company will not pay a replacement cost settlement until the property that was damaged or destroyed is actually repaired or replaced as soon as reasonably possible after the loss.

Under no circumstances will the insurance company pay more than your limit of insurance or more than the actual amount you spend to repair or replace the damaged property if this amount is less than the limit of insurance.

Replacement cost insurance terms give the insured the option of settling the loss on an ACV basis. This option may be exercised if you don’t plan to replace the building or if you are faced with a significant coinsurance penalty on a replacement cost settlement.

References:
http://www.schirickinsurance.com/resources/value2005.pdf
and
TIPTON, Harold F. & KRAUSE, MICKI
Information Security Management Handbook, 4th Edition, Volume 1
Property Insurance overview, Page 587.

QUESTION 253
If your property Insurance has Replacement Cost Valuation (RCV) clause your damaged property will be compensated:

A. Based on the value of item on the date of loss
B. Based on new, comparable, or identical item for old regardless of condition of lost item
C. Based on value of item one month before the loss
D. Based on the value listed on the Ebay auction web site

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
RCV is the maximum amount your insurance company will pay you for damage to covered property before deducting for depreciation. The RCV payment is based on the current cost to replace your property with new, identical or comparable property.

The other choices were detractor:

Application and definition of the insurance terms Replacement Cost Value (RCV), Actual Cash Value (ACV) and depreciation can be confusing. It's important that you understand the terms to help settle your claim fairly.

An easy way to understand RCV and ACV is to think in terms of "new" and "used."
Replacement cost is the item's current price, new. "What will it cost when I replace it?"
Actual cash is the item's used price, old. "How much money is it worth since I used it for five years?"

Hold Back
Most policies only pay the Actual Cash Value upfront, and then they pay you the "held back" depreciation after you incur the expense to repair or replace your personal property items.

NOTE: You must remember to send documentation to the insurance company proving you've incurred the additional expense you will be reimbursed.

Actual Cash Value (ACV)

ACV is the amount your insurance company will pay you for damage to covered property after deducting for depreciation. ACV is the replacement cost of a new item, minus depreciation. If stated as a simple equation, ACV could be defined as follows: ACV=RCV-Depreciation

Unfortunately, ACV is not always as easy to agree upon as a simple math equation. The ACV can also be calculated as the price a willing buyer would pay for your used item.

Depreciation
Depreciation (sometimes called “hold back”) is defined as the “loss in value from all causes, including age, and wear and tear.” Although the definition seems to be clear, in our experience, value” as a real-world application is clearly subjective and varies widely. We have seen the same adjuster apply NO depreciation (100 percent value) on one claim and 40 percent depreciation almost half value) on an almost identical claim.

This shows that the process of applying depreciation is subjective and clearly negotiable.

Excessive Depreciation
When the insurance company depreciates more than they should, it is called “Excessive depreciation.” Although not ethical, it is very common. Note any items that have excessive depreciation and write a letter to your insurance company.

References:
http://carehelp.org/downloads/category/1-insurance-handouts.html?download=17%3Ahandout08-rcv-and-acv
and
http://www.schirickinsurance.com/resources/value2005.pdf
and
TIPTON, Harold F. & KRAUSE, MICKI, information Security Management Handbook, 4th Edition, Volume 1
Property Insurance overview, Page 587.

QUESTION 254
A momentary power outage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

A momentary power outage is a fault.

Power Excess
Spike --> Too much voltage for a short period of time.
Surge --> Too much voltage for a long period of time.

Power Loss
Fault --> A momentary power outage.
Blackout --> A long power interruption.

Power Degradation
Sag or Dip --> A momentary low voltage.
Brownout --> A prolonged power supply that is below normal voltage.

Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.
and
https://en.wikipedia.org/wiki/Power_quality

QUESTION 255
A momentary high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Too much voltage for a short period of time is a spike.

Too much voltage for a long period of time is a surge.

Not enough voltage for a short period of time is a sag or dip

Not enough voltage for a long period of time is brownout

A short power interruption is a fault

A long power interruption is a blackout

You MUST know all of the power issues above for the purpose of the exam.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

QUESTION 256
Which of the following items is NOT a benefit of cold sites?

A. No resource contention with other organisation
B. Quick Recovery
C. A secondary location is available to reconstruct the environment
D. Low Cost

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A cold site is a permanent location that provide you with your own space that you can move into in case of a disaster or catastrophe. It is one of the cheapest solution available as a rental place but it is also the one that would take the most time to recover. A cold site usually takes one to two weeks for recoverey.

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. The plan should include a trategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

Dedicated site owned or operated by the organization. Also called redundant or alternate sites;
Reciprocal agreement or memorandum of agreement with an internal or external entity; and
Commercially leased facility.

Regardless of the type of alternate site chosen, the facility must be able to support system operations as defined in the contingency plan. The three alternate site types commonly categorized in terms of their operational readiness are cold sites, warm sites, or hot sites. Other variations or combinations of these can be found, but generally all variations retain similar core features found in one of these three site types.

Progressing from basic to advanced, the sites are described below:

Cold Sites are typically facilities with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support information system recovery activities.

ƒWarm Sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources.

Hot Sites are facilities appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel.

As discussed above, these three alternate site types are the most common. There are also variations, and hybrid mixtures of features from any one of the three. Each organization should evaluate its core requirements in order to establish the most effective solution.

Two examples of variations to the site types are:

ƒMobile Sites are self-contained, transportable shells custom-fitted with specific telecommunications and system equipment necessary to meet system requirements. ƒMirrored Sites are fully redundant facilities with automated real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects.

There are obvious cost and ready-time differences among the options. In these examples, the mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain, although they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. In many cases, mobile sites may be delivered to the desired location within 24 hours, but the time necessary for equipment installation and setup can increase this response time. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel and/or equipment there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same hazard as the organization's primary site.

The following reference(s) were used for this question:
http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

QUESTION 257
Qualitative loss resulting from the business interruption does NOT usually include:

A. Loss of revenue
B. Loss of competitive advantage or market share
C. Loss of public confidence and credibility
D. Loss of market leadership

Correct Answer: A
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
This question is testing your ability to evaluate whether items on the list are Qualitative or Quantitative. All of the items listed were Qualitative except Lost of Revenue which is Quantitative.

Those are mainly two approaches to risk analysis, see a description of each below:

A quantitative risk analysis is used to assign monetary and numeric values to all elements of the risk analysis process. Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks. It is more of a scientific or mathematical approach to risk analysis compared to qualitative.

A qualitative risk analysis uses a “softer” approach to the data elements of a risk analysis . It does not quantify that data, which means that it does not assign numeric values to the data so that they can be used in equations.

Qualitative and quantitative impact information should be gathered and then properly analyzed and interpreted. The goal is to see exactly how a business will be affected by different threats.

The effects can be economical, operational, or both. Upon completion of the data analysis, it should be reviewed with the most knowledgeable people within the company to ensure that the findings are appropriate and that it describes the real risks and impacts the organization faces. This will help flush out any additional data points not originally obtained and will give a fuller understanding of all the possible business impacts.

Loss criteria must be applied to the individual threats that were identified. The criteria may include the following:

Loss in reputation and public confidence
Loss of competitive advantages
Increase in operational expenses
Violations of contract agreements
Violations of legal and regulatory requirements
Delayed income costs
Loss in revenue
Loss in productivity

Reference used for this question:
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 909). McGraw-Hill. Kindle Edition.

QUESTION 258
When you update records in multiple locations or you make a copy of the whole database at a remote location as a way to achieve the proper level of fault-tolerance and redundancy, it is knows as?

A. Shadowing
B. Data mirroring
C. Backup
D. Archiving

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Updating records in multiple locations or copying an entire database to a remote location as a means to ensure the appropriate levels of fault-tolerance and redundancy is known as Database shadowing. Shadowing is the technique in which updates are shadowed in multiple locations. It is like copying the entire database on to a remote location.

Shadow files are an exact live copy of the original active database, allowing you to maintain live duplicates of your production database, which can be brought into production in the event of a hardware failure. They are used for security reasons: should the original database be damaged or incapacitated by hardware problems, the shadow can immediately take over as the primary database. It is therefore important that shadow files do not run on the same server or at least on the same drive as the primary database files.

The following are incorrect answers:

Data mirroring In data storage, disk mirroring is the replication of logical disk volumes onto separate physical hard disks in real time to ensure continuous availability. It is most commonly used in RAID 1. A mirrored volume is a complete logical representation of separate volume copies.

Backups In computing the phrase backup means to copy files to a second medium (a disk or tape) as a precaution in case the first medium fails. One of the cardinal rules in using computers is back up your files regularly. Backups are useful in recovering information or a system in the event of a disaster, else you may be very sorry :-(

Archiving is the storage of data that is not in continual use for historical purposes. It is the process of copying files to a long-term storage medium for backup.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 27614-27626). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Disk_mirroring
http://www.webopedia.com/TERM/A/archive.html
http://ibexpert.net/ibe/index.php?n=Doc.DatabaseShadow

QUESTION 259
Recovery Site Strategies for the technology environment depend on how much downtime an organization can tolerate before the recovery must be completed. What would you call a strategy where the alternate site is internal, standby ready, with all the technology and equipment necessary to run the applications?

A. External Hot site
B. Warm Site
C. Internal Hot Site

D. Dual Data Center

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Internal Hot Site—This site is standby ready with all the technology and equipment necessary to run the applications positioned there. The planner will be able to effectively restart an application in a hot site recovery without having to perform any bare metal recovery of servers. If this is an internal solution, then often the organization will run non-time sensitive processes there such as development or test environments, which will be pushed aside for recovery of production when needed. When employing this strategy, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery.
Recovery Site Strategies Depending on how much downtime an organization has before the technology recovery must be complete, recovery strategies selected for the technology environment could be any one of the following:
Dual Data Center—This strategy is employed for applications, which cannot accept any downtime without negatively impacting the organization. The applications are split between two geographically dispersed data centers and either load balanced between the two centers or hot swapped between the two centers. The surviving data center must have enough head room to carry the full production load in either case.

External Hot Site—This strategy has equipment on the floor waiting, but the environment must be rebuilt for the recovery. These are services contracted through a recovery service provider. Again, it is important that the two environments be kept as close to identical as possible to avoid problems with O/S levels, hardware differences, capacity differences, etc., from preventing or delaying recovery. Hot site vendors tend to have the most commonly used hardware and software products to attract the largest number of customers to utilize the site. Unique equipment or software would generally need to be provided by the organization either at time of disaster or stored there ahead of time.
Warm Site—A leased or rented facility that is usually partially configured with some equipment, but not the actual computers. It will generally have all the cooling, cabling, and networks in place to accommodate the recovery but the actual servers, mainframe, etc., equipment are delivered to the site at time of disaster.
Cold Site—A cold site is a shell or empty data center space with no technology on the floor. All technology must be purchased or acquired at the time of disaster.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21265-21291). Auerbach Publications. Kindle Edition.

QUESTION 260
What is the most correct choice below when talking about the steps to resume normal operation at the primary site after the green light has been given by the salvage team?

A. The most critical operations are moved from alternate site to primary site before others
B. Operation may be carried by a completely different team than disaster recovery team
C. The least critical functions should be moved back first

D. You moves items back in the same order as the categories document in your plan or exactly in the same order as you did on your way to the alternate site

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
It's interesting to note that the steps to resume normal processing operations will be different than the steps of the recovery plan; that is, the least critical work should be brought back first to the primary site.

The most important point above in the steps would be to move the least critical items or resources back to the primary site first. This way you can ensure that the site was really well prepared and that all is working fine.

Before that first step would be done, you would get the green light from the salvage team that it is fine to move back to the primary site. The first step after getting the green light would be to move the least critical elements first.

As stated in the Shon Harris book:
The least critical functions should be moved back first, so if there are issues in network configurations or connectivity, or important steps were not carried out, the critical operations of the company are not negatively affected. Why go through the trouble of moving the most critical systems and operations to a safe and stable site, only to return it to a main site that is untested? Let the less critical departments act as the canary. If they survive, then move over the more critical components of the company.

When it is time for the company to move back into its original site or a new site, the company enters the reconstitution phase. A company is not out of an emergency state until it is back in operation at the original primary site or a new site that was constructed to replace the primary site, because the company is always vulnerable while operating in a backup facility.

Many logistical issues need to be considered as to when a company must return from the alternate site to the original site. The following lists a few of these issues:

Ensuring the safety of employees
Ensuring an adequate environment is provided (power, facility infrastructure, water, HVAC)
Ensuring that the necessary equipment and supplies are present and in working order
Ensuring proper communications and connectivity methods are working
Properly testing the new environment

Once the coordinator, management, and salvage team sign off on the readiness of the facility, the salvage team should carry out the following steps:

Back up data from the alternate site and restore it within the new facility.
Carefully terminate contingency operations.
Securely transport equipment and personnel to the new facility.

All other choices are not the correct answer.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Location 19389). McGraw-Hill. Kindle Edition.
and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Page 290.

QUESTION 261
What would be the Annualized Rate of Occurrence (ARO) of the threat "user input error", in the case where a company employs 100 data entry clerks and every one of them makes one input error each month?

A. 100
B. 120
C. 1
D. 1200

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
If every one of the 100 clerks makes 1 error 12 times per year, it makes a total of 1200 errors. The Annnualized Rate of Occurence (ARO) is a value that represents the estimated frequency in which a threat is expected to occur. The range can be from 0.0 to a large number. Having an average of 1200 errors per year means an ARO of 1200

QUESTION 262
How is Annualized Loss Expectancy (ALE) derived from a threat?

A. ARO x (SLE - EF)
B. SLE x ARO
C. SLE/EF
D. AV x EF

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Three steps are undertaken in a quantitative risk assessment:

Initial management approval
Construction of a risk assessment team, and
The review of information currently available within the organization.

There are a few formulas that you MUST understand for the exam. See them below:

SLE (Single Loss Expectancy)
Single loss expectancy (SLE) must be calculated to provide an estimate of loss. SLE is defined as the difference between the original value and the remaining value of an asset after a single exploit.

The formula for calculating SLE is as follows: SLE = asset value (in $) × exposure factor (loss due to successful threat exploit, as a %)

Losses can include lack of availability of data assets due to data loss, theft, alteration, or denial of service (perhaps due to business continuity or security issues).

ALE (Annualized Loss Expectancy)
Next, the organization would calculate the annualized rate of occurrence (ARO).

This is done to provide an accurate calculation of annualized loss expectancy (ALE).

ARO is an estimate of how often a threat will be successful in exploiting a vulnerability over the period of a year.

When this is completed, the organization calculates the annualized loss expectancy (ALE).
The ALE is a product of the yearly estimate for the exploit (ARO) and the loss in value of an asset after an SLE.

The calculation follows ALE = SLE x ARO

Note that this calculation can be adjusted for geographical distances using the local annual frequency estimate (LAFE) or the standard annual frequency estimate (SAFE). Given that there is now a value for SLE, it is possible to determine what the organization should spend, if anything, to apply a countermeasure for the risk in question.

Remember that no countermeasure should be greater in cost than the risk it mitigates, transfers, or avoids.
Countermeasure cost per year is easy and straightforward to calculate. It is simply the cost of the countermeasure divided by the years of its life (i.e., use within the organization). Finally, the organization is able to compare the cost of the risk versus the cost of the countermeasure and make some objective decisions regarding its countermeasure selection.

The following were incorrect answers:

All of the other choices were incorrect.

The following reference(s) were used for this quesiton:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 10048-10069). Auerbach Publications. Kindle Edition.

QUESTION 263
What does "residual risk" mean?

A. The security risk that remains after controls have been implemented

B. Weakness of an assets which can be exploited by a threat
C. Risk that remains after risk assessment has has been performed
D. A security risk intrinsic to an asset being audited, where no mitigation has taken place.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Residual risk is "The security risk that remains after controls have been implemented" ISO/IEC TR 13335-1 Guidelines for the Management of IT Security (GMITS), Part 1: Concepts and Models for IT Security, 1996. "Weakness of an assets which can be exploited by a threat" is vulnerability. "The result of unwanted incident" is impact. Risk that remains after risk analysis has been performed is a distracter.

Risk can never be eliminated nor avoided, but it can be mitigated, transferred or accpeted. Even after applying a countermeasure like for example putiing up an Antivirus. But still it is not 100% that systems will be protected by antivirus.

QUESTION 264
Business Continuity and Disaster Recovery Planning (Primarily) addresses the:

A. Availability of the CIA triad
B. Confidentiality of the CIA triad
C. Integrity of the CIA triad
D. Availability, Confidentiality and Integrity of the CIA triad

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Information Technology (IT) department plays a very important role in identifying and protecting the company's internal and external information dependencies. Also, the information technology elements of the BCP should address several vital issue, including:

Ensuring that the company employs sufficient physical security mechanisms to preserve vital network and hardware components. including file and print servers.
Ensuring that the organization uses sufficient logical security methodologies (authentication, authorization, etc.) for sensitive data.

Reference: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 279.

QUESTION 265
What is called an event or activity that has the potential to cause harm to the information systems or networks?

A. Vulnerability
B. Threat agent
C. Weakness
D. Threat

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 266
A weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks is called a ?

A. Vulnerability
B. Risk
C. Threat
D. Overflow

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Answer: Vulnerability; Vulnerability is a weakness or lack of a safeguard, which may be exploited by a threat, causing harm to the information systems or networks.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 267
What is called the probability that a threat to an information system will materialize?

A. Threat
B. Risk

C. Vulnerability
D. Hole

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Answer: Risk: The potential for harm or loss to an information system or network; the probability that a threat will materialize.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 16, 32.

QUESTION 268
Risk mitigation and risk reduction controls for providing information security are classified within three main categories, which of the following are being used?

A. preventive, corrective, and administrative

B. detective, corrective, and physical
C. Physical, technical, and administrative
D. Administrative, operational, and logical

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Security is generally defined as the freedom from danger or as the condition of safety. Computer security, specifically, is the protection of data in a system against unauthorized disclosure, modification, or destruction and protection of the computer system itself against unauthorized use, modification, or denial of service. Because certain computer security controls inhibit productivity, security is typically a compromise toward which security practitioners, system users, and system operations and administrative personnel work to achieve a satisfactory balance between security and productivity.

Controls for providing information security can be physical, technical, or administrative.
These three categories of controls can be further classified as either preventive or detective. Preventive controls attempt to avoid the occurrence of unwanted events, whereas detective controls attempt to identify unwanted events after they have occurred. Preventive controls inhibit the free use of computing resources and therefore can be applied only to the degree that the users are willing to accept. Effective security awareness programs can help increase users' level of tolerance for preventive controls by helping them understand how such controls enable them to trust their computing systems. Common detective controls include audit trails, intrusion detection methods, and checksums.

Three other types of controls supplement preventive and detective controls. They are usually described as deterrent, corrective, and recovery.

Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures. These usually take the form of constraints that make it difficult or undesirable to perform unauthorized activities or threats of consequences that influence a potential intruder to not violate security (e.g., threats ranging from embarrassment to severe punishment).
Corrective controls either remedy the circumstances that allowed the unauthorized activity or return conditions to what they were before the violation. Execution of corrective controls could result in changes to existing physical, technical, and administrative controls.
Recovery controls restore lost computing resources or capabilities and help the organization recover monetary losses caused by a security violation.

Deterrent, corrective, and recovery controls are considered to be special cases within the major categories of physical, technical, and administrative controls; they do not clearly belong in either preventive or detective categories. For example, it could be argued that deterrence is a form of prevention because it can cause an intruder to turn away; however, deterrence also involves detecting violations, which may be what the intruder fears most. Corrective controls, on the other hand, are not preventive or detective, but they are clearly linked with technical controls when antiviral software eradicates a virus or with administrative controls when backup procedures enable restoring a damaged data base. Finally, recovery controls are neither preventive nor detective but are included in administrative controls as disaster recovery or contingency plans.

Reference(s) used for this question

Handbook of Information Security Management, Hal Tipton

QUESTION 269
In the course of responding to and handling an incident, you work on determining the root cause of the incident. In which step are you in?

A. Recovery
B. Containment
C. Triage
D. Analysis and tracking

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
In this step, your main objective is to examine and analyze what has occurred and focus on determining the root cause of the incident.

Recovery is incorrect as recovery is about resuming operations or bringing affected systems back into production

Containment is incorrect as containment is about reducing the potential impact of an incident.

Triage is incorrect as triage is about determining the seriousness of the incident and filtering out false positives

Reference:
Official Guide to the CISSP CBK, pages 700-704

QUESTION 270
Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?

A. Anomaly detection tends to produce more data
B. A pattern matching IDS can only identify known attacks
C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
D. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

This is wrong which makes this the correct choice. This statement is not true as stateful matching scans for attack signatures by analyzing traffic streams rather than individual packets. Stateful matching intrusion detection takes pattern matching to the next level.

As networks become faster there is an emerging need for security analysis techniques that can keep up with the increased network throughput. Existing networkbased intrusion detection sensors can barely keep up with bandwidths of a few hundred Mbps. Analysis tools that can deal with higher throughput are unable to maintain state between different steps of an attack or they are limited to the analysis of packet headers.

The following answers are all incorrect:

Anomaly detection tends to produce more data is true as an anomaly-based IDS produces a lot of data as any activity outside of expected behavior is recorded.

A pattern matching IDS can only identify known attacks is true as a pattern matching IDS works by comparing traffic streams against signatures. These signatures are created for known attacks.

An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines is true as the assertion is a characteristic of a statistical anomaly-based IDS.

Reference:
Official guide to the CISSP CBK. Pages 198 to 201
http://cs.ucsb.edu/~vigna/publications/2003_vigna_robertson_kher_kemmerer_ACSAC03.pdf

QUESTION 271
The IP header contains a protocol field. If this field contains the value of 51, what type of data is contained within the ip datagram?

A. Transmission Control Protocol (TCP)
B. Authentication Header (AH)
C. User datagram protocol (UDP)
D. Internet Control Message Protocol (ICMP)

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
TCP has the value of 6
UDP has the value of 17
ICMP has the value of 1

Reference:

SANS http://www.sans.org/resources/tcpip.pdf?ref=3871

QUESTION 272
Which of the following is NOT a correct notation for an IPv6 address?

A. 2001:0db8:0:0:0:0:1428:57ab
B. ABCD:EF01:2345:6789:ABCD:EF01:2345:6789
C. ::1
D. 2001:DB8::8:800::417A

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
This is not a correct notation for an IPv6 address because the the "::" can only appear once in an address. The use of "::" is a shortcut notation that indicates one or more groups of 16 bits of zeros.

::1 is the loopback address using the special notation
Reference: IP Version 6 Addressing Architecture
http://tools.ietf.org/html/rfc4291#section-2.1 **QUESTION 273**
Another example of Computer Incident Response Team (CIRT) activities is:

A. Management of the netware logs, including collection, retention, review, and analysis of data
B. Management of the network logs, including collection and analysis of data
C. Management of the network logs, including review and analysis of data
D. Management of the network logs, including collection, retention, review, and analysis of data

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Additional examples of CIRT activities are:

Management of the network logs, including collection, retention, review, and analysis of data
Management of the resolution of an incident, management of the remediation of a vulnerability, and post-event reporting to the appropriate parties.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 64.

QUESTION 274
Which of the following backup methods makes a complete backup of every file on the server every time it is run?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Full Backup Method makes a complete backup of every file on the server every time it is run.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 275
Which of the following backup methods is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets?

A. full backup method.
B. incremental backup method.
C. differential backup method.
D. tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Full Backup Method is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 276
Which backup method usually resets the archive bit on the files after they have been backed up?

A. Incremental backup method.
B. Differential backup method.

C. Partial backup method.
D. Tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The incremental backup method usually resets the archive bit on the files after they have been backed up.

An Incremental Backup will backup all the files that have changed since the last Full Backup (the first time it is run after a full backup was previously completed) or after an Incremental Backup (for the second backup and subsequent backups) and sets the archive bit to 0. This type of backup take less time during the backup phase but it will take more time to restore.

The other answers are all incorrect choices.

The following backup types also exists:
Full Backup - All data are backed up. The archive bit is cleared, which means that it is set to 0.
Differential Backup - Backup the files that have been modified since the last Full Backup. The archive bit does not change. Take more time while the backup phase is performed and take less time to restore.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 277
Which backup method is used if backup time is critical and tape space is at an extreme premium?

A. Incremental backup method.
B. Differential backup method.
C. Full backup method.
D. Tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

Full Backup/Archival Backup - Complete/Full backup of every selected file on the system regardless of whether it has been backup recently.. This is the slowest of the backup methods since it backups all the data. It's however the fastest for restoring data.

Incremental Backup - Any backup in which only the files that have been modified since last full back up are backed up. The archive attribute should be updated while backing up only modified files, which indicates that the file has been backed up. This is the fastest of the backup methods, but the slowest of the restore methods.

Differential Backup - The backup of all data files that have been modified since the last incremental backup or archival/full backup. Uses the archive bit to determine what files have changed since last incremental backup or full backup. The files grows each day until the next full backup is performed clearing the archive attributes. This enables the user to restore all files changed since the last full backup in one pass. This is a more neutral method of backing up data since it's not faster nor slower than the other two

Easy Way To Remember each of the backup type properties:

	Backup Speed	Restore Speed
Full	3	1
Differential	2	2
Incremental	1	3

Legend: 1 = Fastest 2 = Faster 3 = Slowest

Source:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.
and
http://www.proprofs.com/mwiki/index.php/Full_Backup,_Incremental_%26_Differential_Backup

QUESTION 278
Which backup method copies only files that have changed since the last full backup, but does not clear the archive bit?

A. Differential backup method.
B. Full backup method.
C. Incremental backup method.
D. Tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

One of the key item to understand regarding backup is the archive bit. The archive bit is used to determine what files have been backuped already. The archive bit is set if a file is modified or a new file is created, this indicates to the backup program that it has to be saved on the next backup. When a full backup is performed the archive bit will be cleared indicating that the files were backup. This allows backup programs to do an incremental or differential backup that only backs up the changes to the filesystem since the last time the bit was cleared Full Backup (or Reference Backup)
A Full backup will backup all the files and folders on the drive every time you run the full backup. The archive bit is cleared on all files indicating they were all backuped.

Advantages:
All files from the selected drives and folders are backed up to one backup set.
In the event you need to restore files, they are easily restored from the single backup set.

Disadvantages:
A full backup is more time consuming than other backup options.
Full backups require more disk, tape, or network drive space.
Incremental Backup
An incremental backup provides a backup of files that have changed or are new since the last incremental backup.

For the first incremental backup, all files in the file set are backed up (just as in a full backup). If you use the same file set to perform a incremental backup later, only the files that have changed are backed up. If you use the same file set for a third backup, only the files that have changed since the second backup are backed up, and so on.

Incremental backup will clear the archive bit.
Advantages:
Backup time is faster than full backups.
Incremental backups require less disk, tape, or network drive space.
You can keep several versions of the same files on different backup sets.
Disadvantages:

In order to restore all the files, you must have all of the incremental backups available.
It may take longer to restore a specific file since you must search more than one backup set to find the latest version of a file.
Differential Backup

A differential backup provides a backup of files that have changed since a full backup was performed. A differential backup typically saves only the files that are different or new since the last full backup. Together, a full backup and a differential backup include all the files on your computer, changed and unchanged.

Differential backup do not clear the archive bits.

Advantages:

Differential backups require even less disk, tape, or network drive space than incremental backups. Backup time is faster than full or incremental backups. Disadvantages:
Restoring all your files may take considerably longer since you may have to restore both the last differential and full backup. Restoring an individual file may take longer since you have to locate the file on either the differential or full backup.

For more info see: http://support.microsoft.com/kb/136621
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 279
Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?

A. differential backup method
B. full backup methodC. incremental backup method
D. tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup.
Archive Bits

Unless you've done a lot of backups in your time you've probably never heard of an Archive Bit. An archive bit is, essentially, a tag that is attached to every file. In actuality, it is a binary digit that is set on or off in the file, but that's crummy technical jargon that doesn't really tell us anything. For the sake of our discussion, just think of it as the flag on a mail box. If the flag is up, it means the file has been changed. If it's down, then the file is unchanged.

Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them.
Backup Types

Full or Normal
The "Full" or "normal" backup type is the most standard. This is the backup type that you would use if you wanted to backup every file in a given folder or drive. It backs up everything you direct it to regardless of what the archive bit says. It also resets all archive bits (puts the flags down). Most backup software, including the built-in Windows backup software, lets you select down to the individual file that you want backed up. You can also choose to backup things like the "system state".

Incremental

When you schedule an incremental backup, you are in essence instructing the software to only backup files that have been changed, or files that have their flag up. After the incremental backup of that file has occured, that flag will go back down. If you perform a normal backup on Monday, then an incremental backup on Wednesday, the only files that will be backed up are those that have changed since Monday. If on Thursday someone deletes a file by accident, in order to get it back you will have to restore the full backup from Monday, followed by the Incremental backup from Wednesday.

Differential
Differential backups are similar to incremental backups in that they only backup files with their archive bit, or flag, up. However, when a differential backup occurs it does not reset those archive bits which means, if the following day, another differential backup occurs, it will back up that file again regardless of whether that file has been changed or not.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617619).
And: http://www.brighthub.com/computing/windows-platform/articles/24531.aspx

QUESTION 280
Which of the following backup method must be made regardless of whether Differential or Incremental methods are used?

A. Full Backup Method.
B. Incremental backup method.
C. Supplemental backup method.
D. Tape backup method.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A Full Backup must be made regardless of whether Differential or Incremental methods are used.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

And: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (pages 617619).

QUESTION 281
Which of the following tape formats can be used to backup data systems in addition to its original intended audio uses?

A. Digital Video Tape (DVT).
B. Digital Analog Tape (DAT).
C. Digital Voice Tape (DVT).
D. Digital Audio Tape (DAT).

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Digital Audio Tape (DAT) can be used to backup data systems in addition to its original intended audio uses.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 70.

QUESTION 282
Which of the following is NOT a common category/classification of threat to an IT system?

A. Human
B. Natural
C. Technological
D. Hackers

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Hackers are classified as a human threat and not a classification by itself.

All the other answers are incorrect. Threats result from a variety of factors, although they are classified in three types: Natural (e.g., hurricane, tornado, flood and fire), human (e.g. operator error, sabotage, malicious code) or technological (e.g. equipment failure, software error, telecommunications network outage, electric power failure).

Reference:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errataNov11-2010.pdf, June 2002 (page 6).

QUESTION 283

Which of the following enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks?

A. Risk assessment
B. Residual risks
C. Security controls
D. Business units

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The risk assessment is critical because it enables the person responsible for contingency planning to focus risk management efforts and resources in a prioritized manner only on the identified risks. The risk management process includes the risk assessment and determination of suitable technical, management, and operational security controls based on the level of threat the risk imposes. Business units should be included in this process.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION 284
A contingency plan should address:

A. Potential risks. B.
Residual risks.
C. Identified risks.
D. All answers are correct.

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Because it is rarely possible or cost effective to eliminate all risks, an attempt is made to reduce risks to an acceptable level through the risk assessment process. This process allows, from a set of potential risks (whether likely or not), to come up with a set of identified, possible risks.

The implementation of security controls allows reducing the identified risks to a smaller set of residual risks. Because these residual risks represent the complete set of situations that could affect system performance, the scope of the contingency plan may be reduced to address only this decreased risk set.

As a result, the contingency plan can be narrowly focused, conserving resources while ensuring an effective system recovery capability.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 7).

QUESTION 285
Which of the following focuses on sustaining an organization's business functions during and after a disruption?

A. Business continuity plan
B. Business recovery plan
C. Continuity of operations plan
D. Disaster recovery plan

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A business continuity plan (BCP) focuses on sustaining an organization's business functions during and after a disruption. Information systems are considered in the BCP only in terms of their support to the larger business processes. The business recovery plan (BRP) addresses the restoration of business processes after an emergency. The BRP is similar to the BCP, but it typically lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. The continuity of operations plan (COOP) focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. The disaster recovery plan (DRP) applies to major, usually catastrophic events that deny access to the normal facility for an extended period. A DRP is narrower in scope than an IT contingency plan in that it does not address minor disruptions that do not require relocation.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 286
Which of the following specifically addresses cyber attacks against an organization's IT systems?

A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software. The continuity of support plan is the same as an IT contingency plan. It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 287
In which of the following phases of system development life cycle (SDLC) is contingency planning most important?

A. Initiation
B. Development/acquisition
C. Implementation
D. Operation/maintenance

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Contingency planning requirements should be considered at every phase of SDLC, but most importantly when a new IT system is being conceived. In the initiation phase, system requirements are identified and matched to their related operational processes, allowing determination of the system's appropriate recovery priority.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 12).
and
The Official ISC2 Guide to the CBK, Second Edition, Application Security, page 180-185

QUESTION 288
Which of the following teams should NOT be included in an organization's contingency plan?

A. Damage assessment team
B. Hardware salvage team

C. Tiger team
D. Legal affairs team

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 289
Which of the following statements pertaining to the maintenance of an IT contingency plan is incorrect?

A. The plan should be reviewed at least once a year for accuracy and completeness.
B. The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.
C. Strict version control should be maintained.
D. Copies of the plan should be provided to recovery personnel for storage offline at home and office.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled.
Not all employees would obtain a copy, but only those involved in the execution of the plan.
All other statements are correct.

NOTE FROM CLEMENT:

I have received multiple emails stating the explanations contradict the correct answer. It seems many people have a hard time with negative question. In this case the Incorrect choice (the one that is not true) is the correct choice. Be very carefull of such questions, you will get some on the real exam as well.

Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 290
Which of the following is less likely to accompany a contingency plan, either within the plan itself or in the form of an appendix?

A. Contact information for all personnel.
B. Vendor contact information, including offsite storage and alternate site.
C. Equipment and system requirements lists of the hardware, software, firmware and other resources required to support system operations.
D. The Business Impact Analysis.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Why is this the correct answer? Simply because it is WRONG, you would have contact information for your emergency personnel within the plan but NOT for ALL of your personnel. Be careful of words such as ALL.
According to NIST's Special publication 800-34, contingency plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management contingency requirements of the given system. Contact information for recovery team personnel (not all personnel) and for vendor should be included, as well as detailed system requirements to allow for supporting of system operations. The Business Impact Analysis (BIA) should also be included as an appendix for reference should the plan be activated.

Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 291
Which of the following server contingency solutions offers the highest availability?

A. System backups
B. Electronic vaulting/remote journaling
C. Redundant arrays of independent disks (RAID)
D. Load balancing/disk replication

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Of the offered technologies, load balancing/disk replication offers the highest availability, measured in terms of minutes of lost data or server downtime.
A Network-Attached Storage (NAS) or a Storage Area Network (SAN) solution combined with virtualization would offer an even higher availability.

Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 49).

QUESTION 292
What assesses potential loss that could be caused by a disaster?

A. The Business Assessment (BA)
B. The Business Impact Analysis (BIA)
C. The Risk Assessment (RA)
D. The Business Continuity Plan (BCP)

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The Business Assessment is divided into two components. Risk Assessment (RA) and Business Impact Analysis (BIA). Risk Assessment is designed to evaluate existing exposures from the organization's environment, whereas the BIA assesses potential loss that could be caused by a disaster. The Business Continuity Plan's goal is to reduce the risk of financial loss by improving the ability to recover and restore operations efficiently and effectively.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).
And: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 276).

QUESTION 293
Which of the following item would best help an organization to gain a common understanding of functions that are critical to its survival?

A. A risk assessment
B. A business assessment
C. A disaster recovery plan

D. A business impact analysis

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A Business Impact Analysis (BIA) is an assessment of an organization's business functions to develop an understanding of their criticality, recovery time objectives, and resources needed.

By going through a Business Impact Analysis, the organization will gain a common understanding of functions that are critical to its survival.

A risk assessment is an evaluation of the exposures present in an organization's external and internal environments.
A Business Assessment generally include Business Analysis as a discipline and it has heavy overlap with requirements analysis sometimes also called requirements engineering, but focuses on identifying the changes to an organization that are required for it to achieve strategic goals. These changes include changes to strategies, structures, policies, processes, and information systems.
A disaster recovery plan is the comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).

QUESTION 294
What can be defined as the maximum acceptable length of time that elapses before the unavailability of the system severely affects the organization?

A. Recovery Point Objectives (RPO)
B. Recovery Time Objectives (RTO)
C. Recovery Time Period (RTP)
D. Critical Recovery Time (CRT)

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
One of the results of a Business Impact Analysis is a determination of each business function's Recovery Time Objectives (RTO). The RTO is the amount of time allowed for the recovery of a business function. If the RTO is exceeded, then severe damage to the organization would result.
The Recovery Point Objectives (RPO) is the point in time in which data must be restored in order to resume processing.

Reference(s) used for this question:

BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 68).
and
And: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 47).

QUESTION 295
Which of the following steps should be one of the first step performed in a Business Impact Analysis (BIA)?

A. Identify all CRITICAL business units within the organization.
B. Evaluate the impact of disruptive events.
C. Estimate the Recovery Time Objectives (RTO).
D. Identify and Prioritize Critical Organization Functions

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Project Initiation and Management

This is the first step in building the Business Continuity program is project initiation and management. During this phase, the following activities will occur:

Obtain senior management support to go forward with the project
Define a project scope, the objectives to be achieved, and the planning assumptions
Estimate the project resources needed to be successful, both human resources and financial resources
Define a timeline and major deliverables of the project In this phase, the program will be managed like a project, and a project manager should be assigned to the BC and DR domain.

The next step in the planning process is to have the planning team perform a BIA. The BIA will help the company decide what needs to be recovered, and how quickly. Mission functions are typically designated with terms such as critical, essential, supporting and nonessential to help determine the appropriate prioritization.

One of the first steps of a BIA is to Identify and Prioritize Critical Organization Functions. All organizational functions and the technology that supports them need to be classified based on their recovery priority. Recovery time frames for organization operations are driven by the consequences of not performing the function. The consequences may be the result of organization lost during the down period; contractual commitments not met resulting in fines or lawsuits, lost goodwill with customers.

All other answers are incorrect.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 21073-21075). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20697-20710). Auerbach Publications. Kindle Edition.

QUESTION 296
A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern in the context of what your Disaster Recovery Plan would include?

A. Marketing/Public relations
B. Data/Telecomm/IS facilities
C. IS Operations
D. Facilities security

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The main concern when recovering after a disaster is data, telecomm and IS facilities. Other services, in descending priority order are: IS operations, IS support services, market structure, marketing/public relations, customer service & systems support, market regulation/surveillance, listing, application development, accounting services, facilities, human resources, facilities security, legal and Office of the Secretary, national sales.
Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 129).

QUESTION 297
During the salvage of the Local Area Network and Servers, which of the following steps would normally be performed first?

A. Damage mitigation
B. Install LAN communications network and servers
C. Assess damage to LAN and servers
D. Recover equipment

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

The first activity in every recovery plan is damage assessment, immediately followed by damage mitigation.

This first activity would typically include assessing the damage to all network and server components (including cables, boards, file servers, workstations, printers, network equipment), making a list of all items to be repaired or replaced, selecting appropriate vendors and relaying findings to Emergency Management Team.

Following damage mitigation, equipment can be recovered and LAN communications network and servers can be reinstalled.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 135).

QUESTION 298
Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?

A. In order to facilitate recovery, a single plan should cover all locations.
B. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
C. In its procedures and tasks, the plan should refer to functions, not specific individuals.
D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The first documentation rule when it comes to a BCP/DRP is "one plan, one building". Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

QUESTION 299
A Business Continuity Plan should be tested:

A. Once a month.
B. At least twice a year.
C. At least once a year.

 D. At least

once every two years.

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
It is recommended that testing does not exceed established frequency limits. For a plan to be effective, all components of the BCP should be tested at least once a year. Also, if there is a major change in the operations of the organization, the plan should be revised and tested not more than three months after the change becomes operational.

Source: BARNES, James C. & ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 165).

QUESTION 300

Which of the following statements pertaining to a Criticality Survey is incorrect?

A. It is implemented to gather input from all personnel that is going to be part of the recovery teams.
B. The purpose of the survey must be clearly stated.
C. Management's approval should be obtained before distributing the survey.
D. Its intent is to find out what services and systems are critical to keeping the organization in business.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

The Criticality Survey is implemented through a standard questionnaire to gather input from the most knowledgeable people. Not all personnel that is going to be part of recovery teams is necessarily able to help in identifying critical functions of the organization.

The intent of such a survey is to identify the services and systems that are critical to the organization.

Having a clearly stated purpose for the survey helps in avoiding misinterpretations.

Management's approval of the survey should be obtained before distributing it.
Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 301
Which disaster recovery plan test involves functional representatives meeting to review the plan in detail?

A. Simulation test
B. Checklist test
C. Parallel test
D. Structured walk-through test

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The structured walk-through test occurs when the functional representatives meet to review the plan in detail. This involves a thorough look at each of the plan steps, and the procedures that are invoked at that point in the plan. This ensures that the actual planned activities are accurately described in the plan. The checklist test is a method of testing the plan by distributing copies to each of the functional areas. The simulation test plays out different scenarios. The parallel test is essentially an operational test that is performed without interrupting current processing.

Source: HARE, Chris, CISSP Study Guide: Business Continuity Planning Domain,

QUESTION 302
The criteria for evaluating the legal requirements for implementing safeguards is to evaluate the cost (C) of instituting the protection versus the estimated loss (L) resulting from the exploitation of the corresponding vulnerability. Therefore, a legal liability may exists when:

A. (C < L) or C is less than L
B. (C < L - (residual risk)) or C is less than L minus residual risk
C. (C > L) or C is greather than L
D. (C > L - (residual risk)) or C is greather than L minus residual risk

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
If the cost is lower than the estimated loss (C < L), then legal liability may exists if you fail to implement the proper safeguards.

Government laws and regulations require companies to employ reasonable security measures to reduce private harms such as identity theft due to unauthorized access. The U.S. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule and the broader European Directive 95/46/EC, Article 17, both require that companies employ reasonable or appropriate administrative and technical security measures to protect consumer information.

The GLBA is a U.S. Federal law enacted by U.S. Congress in 1998 to allow consolidation among commercial banks. The GLBA Safeguards Rule is U.S. Federal regulation created in reaction to the GLBA and enforced by the U.S.
Federal Trade Commission (FTC). The Safeguards Rule requires companies to implement a security plan to protect the confidentiality and integrity of consumer personal information and requires the designation of an individual responsible for compliance.

Because these laws and regulations govern consumer personal information, they can lead to new requirements for information systems for which companies are responsible to comply.

The act of compliance includes demonstrating due diligence, which is defined as "reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations". Reasonableness in software systems includes industries standards and may allow for imperfection. Lawyers representing firms and other organizations, regulators, system administrators and engineers all face considerable challenge in determining what constitutes "reasonable" security measures for several reasons, including:

1. Compliance changes with the emergence of new security vulnerabilities due to innovations in information technology;

2. Compliance requires knowledge of specific security measures, however publicly available best practices typically include general goals and only address broad categories of vulnerability; and

3. Compliance is a best-effort practice, because improving security is costly and companies must prioritize security spending commensurate with risk of noncompliance. In general, the costs of improved security are certain, but the improvement in security depends on unknown variables and probabilities outside the control of companies.

The following reference(s) were used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 315.
and http://www.cs.cmu.edu/~breaux/publications/tdbreaux-cose10.pdf

QUESTION 303

What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

A. Evidence Circumstance Doctrine
B. Exigent Circumstance Doctrine
C. Evidence of Admissibility Doctrine
D. Exigent Probable Doctrine

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances.

For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child. Examples of other exigent circumstances include protecting evidence or property from imminent destruction.

In US v Martinez, Justice Thomas of the United States Court of Appeal used these words:

"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."

In Alvarado, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust:

"The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required."

All of the other answers were only detractors made up and not legal terms.

Reference(s) used for this question:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 313.
and
http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx

QUESTION 304

A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

A. Direct evidence
B. Circumstantial evidence
C. Hearsay evidence
D. Secondary evidence

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Secondary evidence is a copy of evidence or oral description of its contents; not as reliable as best evidence

Here are other types of evidence:
Best evidence — original or primary evidence rather than a copy of duplicate of the evidence

Direct evidence — proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses

Conclusive evidence — incontrovertible; overrides all other evidence

Opinions — two types: Expert — may offer an opinion based on personal expertise and facts, Non-expert — may testify only as to facts

Circumstantial evidence — inference of information from other, immediate, relevant facts

Corroborative evidence — supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence

Hearsay evidence (3rdparty) — oral or written evidence that is presented in court that is second hand and has no firsthand proof of accuracy or reliability
(i) Usually not admissible in court
(ii)Computer generated records and other business records are in hearsay category (iii) Certain exceptions to hearsay rule:
(1) Made during the regular conduct of business and authenticated by witnesses familiar with their use

(2) Relied upon in the regular course of business
(3) Made by a person with knowledge of records
(4) Made by a person with information transmitted by a person with knowledge
(5) Made at or near the time of occurrence of the act being investigated
(6) In the custody of the witness on a regular basis

Reference:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 310.
and
CISSP for Dummies, Peter Gregory, page 270-271

QUESTION 305
Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Direct evidence.
B. Circumstantial evidence.
C. Conclusive evidence.
D. Corroborative evidence.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Direct evidence can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness's five senses.

The following answers are incorrect:

Circumstantial evidence. Is incorrect because Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact.
Conclusive evidence. Is incorrect because Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.

Corroborative evidence. Is incorrect because Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

QUESTION 306
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence
B. Corroborative evidence

C. Opinion evidence
D. Secondary evidence

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. Corrobative evidence takes many forms.

In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and prompt complaint witnesses.

There are many types of evidence that exist. Below you have explanations of some of the most common types:
Physical Evidence

Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.
Real Evidence
Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question.

Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in “the same or substantially the same condition” now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial evidence called chain of custody.

Documentary
Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence

A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication
Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.
The role of the expert witness

Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand. Digital Evidence or Electronic Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.
Demonstrative Evidence
Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.
Chain of custody

Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.

An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence. Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).

Example

An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene:
Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill. Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).

The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible.

In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.

REFERENCES:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.

http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence http://en.wikipedia.org/wiki/Chain_of_custody

QUESTION 307
To understand the 'whys' in crime, many times it is necessary to understand MOM. Which of the following is not a component of MOM?

A. Opportunities
B. Methods
C. Motivation
D. Means

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
To understand the whys in crime, many times it is necessary to understand the Motivations, Opportunities, and Means (MOM). Motivations are the who and why of a crime. Opportunities are the where and when of a crime, and Means pertains to the capabilities a criminal would need to be successful. Methods is not a component of MOM.

QUESTION 308
In the statement below, fill in the blank:

Law enforcement agencies must get a warrant to search and seize an individual's property, as stated in the _____ Amendment.

A. First.
B. Second.
C. Third.
D. Fourth.

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

The Fourth Amendment does not apply to a seizure or an arrest by private citizens.

Search and seizure activities can get tricky depending on what is being searched for and where.
For example, American citizens are protected by the Fourth Amendment against unlawful search and seizure, so law enforcement agencies must have probable cause and request a search warrant from a judge or court before conducting such a search.

The actual search can only take place in the areas outlined by the warrant. The Fourth Amendment does not apply to actions by private citizens unless they are acting as police agents. So, for example, if Kristy's boss warned all employees that the management could remove files from their computers at any time, and her boss was not a police officer or acting as a police agent, she could not successfully claim that her Fourth Amendment rights were violated. Kristy's boss may have violated some specific privacy laws, but he did not violate Kristy's Fourth Amendment rights.

In some circumstances, a law enforcement agent may seize evidence that is not included in the warrant, such as if the suspect tries to destroy the evidence. In other words, if there is an impending possibility that evidence might be destroyed, law enforcement may quickly seize the evidence to prevent its destruction. This is referred to as exigent circumstances, and a judge will later decide whether the seizure was proper and legal before allowing the evidence to be admitted. For example, if a police officer had a search warrant that allowed him to search a suspect's living room but no other rooms, and then he saw the suspect dumping cocaine down the toilet, the police officer could seize the cocaine even though it was in a room not covered under his search warrant. After evidence is gathered, the chain of custody needs to be enacted and enforced to make sure the evidence's integrity is not compromised.

All other choices were only detractors.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1057). McGraw-Hill. Kindle Edition.

QUESTION 309
Controls are implemented to:

A. eliminate risk and reduce the potential for loss
B. mitigate risk and eliminate the potential for loss
C. mitigate risk and reduce the potential for loss
D. eliminate risk and eliminate the potential for loss

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Controls are implemented to mitigate risk and reduce the potential for loss. Preventive controls are put in place to inhibit harmful occurrences; detective controls are established to discover harmful occurrences; corrective controls are used to restore systems that are victims of harmful attacks.

It is not feasible and possible to eliminate all risks and the potential for loss as risk/threats are constantly changing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 32.

QUESTION 310
What can be described as a measure of the magnitude of loss or impact on the value of an asset?

A. Probability

B. Exposure factor
C. Vulnerability
D. Threat

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The exposure factor is a measure of the magnitude of loss or impact on the value of an asset.

The probability is the chance or likelihood, in a finite sample, that an event will occur or that a specific loss value may be attained should the event occur.

A vulnerability is the absence or weakness of a risk-reducing safeguard.
A threat is event, the occurrence of which could have an undesired impact.
Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 3, August 1999.

QUESTION 311
Computer security should be first and foremost which of the following:

A. Cover all identified risks
B. Be cost-effective.
C. Be examined in both monetary and non-monetary terms.
D. Be proportionate to the value of IT systems.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

Computer security should be first and foremost cost-effective.

As for any organization, there is a need to measure their cost-effectiveness, to justify budget usage and provide supportive arguments for their next budget claim. But organizations often have difficulties to accurately measure the effectiveness and the cost of their information security activities.

The classical financial approach for ROI calculation is not particularly appropriate for measuring security-related initiatives: Security is not generally an investment that results in a profit. Security is more about loss prevention. In other terms, when you invest in security, you don't expect benefits; you expect to reduce the risks threatening your assets.

The concept of the ROI calculation applies to every investment. Security is no exception. Executive decision-makers want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know how much is the lack of security costing to the business and what are the most cost-effective solutions.

Applied to security, a Return On Security Investment (ROSI) calculation can provide quantitative answers to essential financial questions:

Is an organization paying too much for its security?
What financial impact on productivity could have lack of security?
When is the security investment enough?
Is this security product/organisation beneficial?

The following are other concerns about computer security but not the first and foremost:
The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits.

Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm.

Requirements for security vary, depending upon the particular IT system. Therefore it does not make sense for computer security to cover all identified risks when the cost of the measures exceeds the value of the systems they are protecting.

Reference(s) used for this question:
SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (page 6). and
http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

QUESTION 312
Which of the following best allows risk management results to be used knowledgeably?

A. A vulnerability analysis
B. A likelihood assessment

C. An uncertainty analysis
D. A threat identification

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. After having performed risk assessment and mitigation, an uncertainty analysis should be performed. Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. A documented uncertainty analysis allows the risk management results to be used knowledgeably. A vulnerability analysis, likelihood assessment and threat identification are all parts of the collection and analysis of data part of the risk assessment, one of the primary activities of risk management.
Source: SWANSON, Marianne & GUTTMAN, Barbara, National Institute of Standards and Technology (NIST), NIST Special Publication 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996 (pages 19-21).

QUESTION 313
What can be best defined as the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment?

A. Risk management
B. Risk analysis
C. Threat analysis
D. Due diligence

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Threat analysis is the examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.

The following answers are incorrect:

Risk analysis is the process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact.

Risk analysis is synonymous with risk assessment and part of risk management, which is the ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve and maintain an acceptable level or risk.

Due Diligence is identifying possible risks that could affect a company based on best practices and standards.

Reference(s) used for this question:
STONEBURNER, Gary & al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page B-3).

QUESTION 314
The first step in the implementation of the contingency plan is to perform:

A. A firmware backup
B. A data backup
C. An operating systems software backup
D. An application software backup

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A data backup is the first step in contingency planning.
Without data, there is nothing to process. "No backup, no recovery".
Backup for hardware should be taken care of next.
Formal arrangements must be made for alternate processing capability in case the need should arise.
Operating systems and application software should be taken care of afterwards.

Source: VALLABHANENI, S. Rao, CISSP Examination Textbooks, Volume 2: Practice, SRV Professional Publications, 2002, Chapter 8, Business Continuity Planning & Disaster Recovery Planning (page 506).

QUESTION 315
The MOST common threat that impacts a business's ability to function normally is:

A. Power Outage
B. Water Damage
C. Severe Weather

D. Labor Strike

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
The MOST common threat that impacts a business's ability to function normally is power. Power interruption cause more business interruption than any other type of event.

The second most common threat is Water such as flood, water damage from broken pipe, leaky roof, etc...

Threats will be discovered while doing your Threats and Risk Assessments (TRA).
There are three elements of risks: threats, assets, and mitigating factors (countermeasures, safeguards, controls).

A threat is an event or situation that if it occured would affect your business and may even prevent it from functioning normally or in some case functioning at all. Evaluation of threats is done by looking at Likelihood and Impact of possible threat. Safeguards, countermeasures, and controls would be used to bring the threat level down to an acceptable level.

Other common events that can impact a company are:

Weather, cable cuts, fires, labor disputes, transportation mishaps, hardware failure, chemical spills, sabotage.

References:
The Official ISC2 Guide to the CISSP CBK, Second Edition, Page 275-276

QUESTION 316
Failure of a contingency plan is usually:

A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training.

Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

QUESTION 317
When referring to a computer crime investigation, which of the following would be the MOST important step required in order to preserve and maintain a proper chain of custody of evidence:

A. Evidence has to be collected in accordance with all laws and all legal regulations.
B. Law enforcement officials should be contacted for advice on how and when to collect critical information.
C. Verifiable documentation indicating the who, what, when, where, and how the evidence was handled should be available.
D. Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation.

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Two concepts that are at the heart of dealing effectively with digital/electronic evidence, or any evidence for that matter, are the chain of custody and authenticity/ integrity.

The chain of custody refers to the who, what, when, where, and how the evidence was handled—from its identification through its entire life cycle, which ends with destruction or permanent archiving.

Any break in this chain can cast doubt on the integrity of the evidence and on the professionalism of those directly involved in either the investigation or the collection and handling of the evidence. The chain of custody requires following a formal process that is well documented and forms part of a standard operating procedure that is used in all cases, no exceptions.

The following are incorrect answers:
Evidence has to be collected in accordance with all laws and legal regulations. Evidence would have to be collected in accordance with applicable laws and regulations but not necessarily with ALL laws and regulations. Only laws and regulations that applies would be followed.

Law enforcement officials should be contacted for advice on how and when to collect critical information. It seems you failed to do your homework, once you have an incident it is a bit late to do this. Proper crime investigation as well as incident response is all about being prepared ahead of time. Obviously, you are improvising if you need to call law enforcement to find out what to do. It is a great way of contaminating your evidence by mistake if you don't have a well documented processs with clear procedures that needs to be followed.

Log files containing information regarding an intrusion are retained for at least as long as normal business records, and longer in the case of an ongoing investigation. Specific legal requirements exists for log retention and they are not the same as normal business records. Laws such as Basel, HIPPAA, SOX, and others has specific requirements.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23465-23470). Auerbach Publications. Kindle Edition. and
ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (pages 282-285).

QUESTION 318
When should a post-mortem review meeting be held after an intrusion has been properly taken care of?

A. Within the first three months after the investigation of the intrusion is completed.
B. Within the first week after prosecution of intruders have taken place, whether successful or not.
C. Within the first month after the investigation of the intrusion is completed.
D. Within the first week of completing the investigation of the intrusion.

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A post-mortem review meeting should be held with all involved parties within three to five working days of completing the investigation of the intrusion. Otherwise, participants are likely to forget critical information. Even if it enabled an organization to validate the correctness of its chain of custody of evidence, it would not make sense to wait until prosecution is complete because it would take too much time and many cases of intrusion never get to court anyway.
Source: ALLEN, Julia H., The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001, Chapter 7: Responding to Intrusions (page 297).

QUESTION 319
What can be defined as an event that could cause harm to the information systems?

A. A risk
B. A threat
C. A vulnerability
D. A weakness

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
A threat is an event or activity that has the potential to cause harm to the information systems. A risk is the probability that a threat will materialize. A vulnerability, or weakness, is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 1: Access Control Systems (page 32).

QUESTION 320
Most access violations are:

A. Accidental
B. Caused by internal hackers
C. Caused by external hackers
D. Related to Internet

Correct Answer: A
Section: Risk, Response and Recovery
Explanation
Explanation/Reference:
The most likely source of exposure is from the uninformed, accidental or unknowing person, although the greatest impact may be from those with malicious or fraudulent intent.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, Chapter 4: Protection of Information Assets (page 192).

QUESTION 321
A business continuity plan is an example of which of the following?

A. Corrective control
B. Detective control
C. Preventive control
D. Compensating control

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Business Continuity Plans are designed to minimize the damage done by the event, and facilitate rapid restoration of the organization to its full operational capacity. They are for use "after the fact", thus are examples of corrective controls.

Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 273).
and
Conrad, Eric; Misenar, Seth; Feldman, Joshua (2012-09-01). CISSP Study Guide (Kindle Location 8069). Elsevier Science (reference). Kindle Edition.
and

QUESTION 322
When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff
B. Senior business unit management
C. BCP committee
D. Functional business units

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Many elements of a BCP will address senior management, such as the statement of importance and priorities, the statement of organizational responsibility, and the statement of urgency and timing. Executive management staff initiates the project, gives final approval and gives ongoing support. The BCP committee directs the planning, implementation, and tests processes whereas functional business units participate in implementation and testing.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 275).

QUESTION 323
Which of the following statements pertaining to disaster recovery planning is incorrect?

A. Every organization must have a disaster recovery plan
B. A disaster recovery plan contains actions to be taken before, during and after a disruptive event.
C. The major goal of disaster recovery planning is to provide an organized way to make decisions if a disruptive event occurs.
D. A disaster recovery plan should cover return from alternate facilities to primary facilities.

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
It is possible that an organization may not need a disaster recovery plan. An organization may not have any critical processing areas or system and they would be able to withstand lengthy interruptions.

Remember that DRP is related to systems needed to support your most critical business functions.

The DRP plan covers actions to be taken when a disaster occur but DRP PLANNING which is the keywork in the question would also include steps that happen before you use the plan such as development of the plan, training, drills, logistics, and a lot more.

To be effective, the plan would certainly cover before, during, and after the disaster actions.

It may take you a couple years to develop a plan for a medium size company, there is a lot that has to happen before the plan would be actually used in a real disaster scenario. Plan for the worst and hope for the best.

All other statements are true.

NOTE FROM CLEMENT:
Below is a great article on who legally needs a plan which is very much in line with this question. Does EVERY company needs a plan? The legal answer is NO. Some companies, industries, will be required according to laws or regulations to have a plan. A blank statement saying: All companies MUST have a plan would not be accurate. The article below is specific to the USA but similar laws will exist in many other countries.

Some companies such as utilities, power, etc... might also need plan if they have been defined as Critical Infrastructure by the government. The legal side of IT is always very complex and varies in different countries. Always talk to your lawyer to ensure you follow the law of the land :-)

Read the details below:
So Who, Legally, MUST Plan?

With the caveats above, let's cover a few of the common laws where there is a duty to have a disaster recovery plan. I will try to include the basis for that requirement, where there is an implied mandate to do so, and what the difference is between the two Banks and Financial Institutions MUST Have a Plan

The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, Title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA) established the Examination Council (the Council).

The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS); and to make recommendations to promote uniformity in the supervision of financial institutions. In other words, every bank, savings and loan, credit union, and other financial institution is governed by the principles adopted by the Council.

In March of 2003, the Council released its Business Continuity Planning handbook designed to provide guidance and examination procedures for examiners in evaluating financial institution and service provider risk-management processes. Stockbrokers MUST Have a Plan

The National Association of Securities Dealers (NASD) has adopted rules that require all its members to have business continuity plans. The NASD oversees the activities of more than 5,100 brokerage firms, approximately 130,800 branch offices and more than 658,770 registered securities representatives.

As of June 14, 2004, the rules apply to all NASD member firms. The requirements, which are specified in Rule 3510, begin with the following:

3510. Business Continuity Plans. (a) Each member must create and maintain a written business continuity plan identifying procedures relating to an emergency or significant business disruption. Such procedures must be reasonably designed to enable the member to meet its existing obligations to customers. In addition, such procedures must address the member's existing relationships with other broker-dealers and counter-parties. The business continuity plan must be made available promptly upon request to NASD staff.

NOTE:
The rules apply to every company that deals in securities, such as brokers, dealers, and their representatives, it does NOT apply to the listed companies themselves.
Electric Utilities WILL Need a Plan

The disaster recovery function relating to the electric utility grid is presently undergoing a change. Prior to 2005, the Federal Energy Regulatory Commission (FERC) could only coordinate volunteer efforts between utilities. This has changed with the adoption of Title XII of the Energy Policy Act of 2005 (16 U.S.C. 824o). That new law authorizes the FERC to create an Electric Reliability Organization (ERO).
The ERO will have the capability to adopt and enforce reliability standards for "all users, owners, and operators of the bulk power system" in the United States. At this time, FERC is in the process of finalizing the rules for the creation of the ERO. Once the ERO is created, it will begin the process of establishing reliability standards.

It is very safe to assume that the ERO will adopt standards for service restoration and disaster recovery, particularly after such widespread disasters as Hurricane Katrina.
Telecommunications Utilities SHOULD Have Plans, but MIGHT NOT

Telecommunications utilities are governed on the federal level by the Federal Communications Commission (FCC) for interstate services and by state Public Utility Commissions (PUCs) for services within the state.

The FCC has created the Network Reliability and Interoperability Council (NRIC). The role of the NRIC is to develop recommendations for the FCC and the telecommunications industry to "insure [sic] optimal reliability, security, interoperability and interconnectivity of, and accessibility to, public communications networks
and the internet." The NRIC members are senior representatives of providers and users of telecommunications services and products, including telecommunications carriers, the satellite, cable television, wireless and computer industries, trade associations, labor and consumer representatives, manufacturers, research organizations, and government-related organizations.

There is no explicit provision that we could find that says telecommunications carriers must have a Disaster Recovery Plan. As I have stated frequently in this series of articles on disaster recovery, however, telecommunications facilities are tempting targets for terrorism. I have not changed my mind in that regard and urge caution.

You might also want to consider what the liability of a telephone company is if it does have a disaster that causes loss to your organization. In three words: It's not much. The following is the statement used in most telephone company tariffs with regard to its liability:

The Telephone Company's liability, if any, for its gross negligence or willful misconduct is not limited by this tariff. With respect to any other claim or suit, by a customer or any others, for damages arising out of mistakes, omissions, interruptions, delays or errors, or defects in transmission occurring in the course of furnishing services hereunder, the Telephone Company's liability, if any, shall not exceed an amount equivalent to the proportionate charge to the customer for the period of service during which such mistake, omission, interruption, delay, error or defect in transmission or service occurs and continues. (Source, General Exchange Tariff for major carrier)

All Health Care Providers WILL Need a Disaster Recovery Plan
HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, which amended the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act, the Act includes a section, Title II, entitled Administrative Simplification, requiring "Improved efficiency in healthcare delivery by standardizing electronic data interchange, and protection of confidentiality and security of health data through setting and enforcing standards."

The legislation called upon the Department of Health and Human Services (HHS) to publish new rules that will ensure security standards protecting the confidentiality and integrity of "individually identifiable health information," past, present, or future.

The final Security Rule was published by HHS on February 20, 2003 and provides for a uniform level of protection of all health information that is housed or transmitted electronically and that pertains to an individual.

The Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits. It also requires entities to protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI, protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule, and ensure compliance by their workforce.

Required safeguards include application of appropriate policies and procedures, safeguarding physical access to ePHI, and ensuring that technical security measures are in place to protect networks, computers and other electronic devices. Companies with More than 10 Employees

The United States Department of Labor has adopted numerous rules and regulations in regard to workplace safety as part of the Occupational Safety and Health Act. For example, 29 USC 654 specifically requires:

(a) Each employer:

(1) shall furnish to each of his employees employment and a place of employment which are free from recognized hazards that are causing or are likely to cause death or serious physical harm to his employees;

(2) shall comply with occupational safety and health standards promulgated under this Act.

(b) Each employee shall comply with occupational safety and health standards and all rules, regulations, and orders issued pursuant to this Act which are applicable to his own actions and conduct.

Other Considerations or Expensive Research Qs for Lawyers (Sorry, Eddie!)

The Foreign Corrupt Practices Act of 1977
Internal Revenue Service (IRS) Law for Protecting Taxpayer Information
Food and Drug Administration (FDA) Mandated Requirements
Homeland Security and Terrorist Prevention
Pandemic (Bird Flu) Prevention
ISO 9000 Certification
Requirements for Radio and TV Broadcasters
Contract Obligations to Customers
Document Protection and Retention Laws
Personal Identity Theft...and MORE!

Suffice it to say you will need to check with your legal department for specific requirements in your business and industry!

I would like to thank my good friend, Eddie M. Pope, for his insightful contributions to this article, our upcoming book, and my ever-growing pool of lawyer jokes. If you want more information on the legal aspects of recovery planning, Eddie can be contacted at my company or via email at mailto:mempope@tellawcomlabs.com.
(Eddie cannot, of course, give you legal advice, but he can point you in the right direction.)

I hope this article helps you better understand the complex realities of the legal reasons why we plan and wish you the best of luck

See original article at: http://www.informit.com/articles/article.aspx?p=777896

See another interesting article on the subject at: http://www.informit.com/articles/article.aspx?p=677910&seqNum=1

References used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 281).

QUESTION 324
Which of the following statements do not apply to a hot site?

A. It is expensive.
B. There are cases of common overselling of processing capabilities by the service provider.
C. It provides a false sense of security.
D. It is accessible on a first come first serve basis. In case of large disaster it might not be accessible.

Correct Answer: C
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Remember this is a NOT question. Hot sites do not provide a false sense of security since they are the best disaster recovery alternate for backup site that you rent.

A Cold, Warm, and Hot site is always a rental place in the context of the CBK. This is definivily the best choices out of the rental options that exists. It is fully configured and can be activated in a very short period of time.

Cold and Warm sites, not hot sites, provide a false sense of security because you can never fully test your plan.

In reality, using a cold site will most likely make effective recovery impossible or could lead to business closure if it takes more than two weeks for recovery.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 284).

QUESTION 325
What can be defined as a batch process dumping backup data through communications lines to a server at an alternate location?

A. Remote journaling
B. Electronic vaulting
C. Data clustering
D. Database shadowing

Correct Answer: B
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Electronic vaulting refers to the transfer of backup data to an off-site location. This is primarily a batch process of dumping backup data through communications lines to a server at an alternate location.

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

The following are incorrect answers:
Remote journaling refers to the parallel processing of transactions to an alternate site (as opposed to a batch dump process). Journaling is a technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.

Database shadowing uses the live processing of remote journaling, but creates even more redundancy by duplicating the database sets to multiple servers. There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.

Data clustering refers to the classification of data into groups (clusters). Clustering may also be used, although it should not be confused with redundancy. In clustering, two or more “partners” are joined into the cluster and may all provide service at the same time. For example, in an active–active pair, both systems may provide services at any time. In the case of a failure, the remaining partners may continue to provide service but at a decreased capacity.

The following resource(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407 and 20411-20414 and 20375-20377 and 20280-20283). Auerbach Publications. Kindle Edition.

QUESTION 326
Which of the following is the most complete disaster recovery plan test type, to be performed after successfully completing the Parallel test?

A. Full Interruption test
B. Checklist test
C. Simulation test
D. Structured walk-through test

Correct Answer: A
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:

The difference between this and the full-interruption test is that the primary production processing of the business does not stop; the test processing runs in parallel to the real processing. This is the most common type of disaster recovery plan testing.

A checklist test is only considered a preliminary step to a real test.

In a structured walk-through test, business unit management representatives meet to walk through the plan, ensuring it accurately reflects the organization's ability to recover successfully, at least on paper.

A simulation test is aimed at testing the ability of the personnel to respond to a simulated disaster, but not recovery process is actually performed.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 289).

QUESTION 327
Which of the following statements pertaining to disaster recovery is incorrect?

A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate backup processing site.
B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.
C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.
D. When returning to the primary site, the most critical applications should be brought back first.

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.

My explanation: at the point where the primary site is ready to receive operations again, less critical systems should be brought back first because one has to make sure that everything will be running smoothly at the primary site before returning critical systems, which are already operating normally at the recovery site.

This will limit the possible interruption of processing to a minimum for most critical systems, thus making it the best option.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 291).

QUESTION 328

If an employee's computer has been used by a fraudulent employee to commit a crime, the hard disk may be seized as evidence and once the investigation is complete it would follow the normal steps of the Evidence Life Cycle. In such case, the Evidence life cycle would not include which of the following steps listed below?

A. Acquisition collection and identification
B. Analysis
C. Storage, preservation, and transportation
D. Destruction

Correct Answer: D
Section: Risk, Response and Recovery
Explanation

Explanation/Reference:
Unless the evidence is illegal then it should be returned to owner, not destroyed.

The Evidence Life Cycle starts with the discovery and collection of the evidence. It progresses through the following series of states until it is finally returned to the victim or owner:

• Acquisition collection and identification
• Analysis
• Storage, preservation, and transportation
• Presented in court
• Returned to victim (owner)

The Second edition of the ISC2 book says on page 529-530:

Identifying evidence: Correctly identifying the crime scene, evidence, and potential containers of evidence.
Collecting or acquiring evidence: Adhering to the criminalistic principles and ensuring that the contamination and the destruction of the scene are kept to a minimum. Using sound, repeatable, collection techniques that allow for the demonstration of the accuracy and integrity of evidence, or copies of evidence.
Examining or analyzing the evidence: Using sound scientific methods to determine the characteristics of the evidence, conducting comparison for individuation of evidence, and conducting event reconstruction.
Presentation of findings: Interpreting the output from the examination and analysis based on findings of fact and articulating these in a format appropriate for the intended audience (e.g., court brief, executive memo, report).

Note on returning the evidence to the Owner/Victim

The final destination of most types of evidence is back with its original owner. Some types of evidence, such as drugs or drug paraphernalia (i.e., contraband), are destroyed after the trial.

Any evidence gathered during a search, although maintained by law enforcement, is legally under the control of the courts. And although a seized item may be yours and may even have your name on it, it might not be returned to you unless the suspect signs a release or after a hearing by the court. Unfortunately, many victims do not want to go to trial; they just want to get their property back.

Many investigations merely need the information on a disk to prove or disprove a fact in question; thus, there is no need to seize the entire system. Once a schematic of the system is drawn or photographed, the hard disk can be removed and then transported to a forensic lab for copying.

Mirror copies of the suspect disk are obtained using forensic software and then one of those copies can be returned to the victim so that business operations can resume.

Reference(s) used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 309). and
The Official Study Book, Second Edition, Page 529-230

QUESTION 329
What algorithm was DES derived from?

A. Twofish.
B. Skipjack.
C. Brooks-Aldeman.
D. Lucifer.

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
NSA took the 128-bit algorithm Lucifer that IBM developed, reduced the key size to 64 bits and with that developed DES.

The following answers are incorrect:

Twofish. This is incorrect because Twofish is related to Blowfish as a possible replacement for DES.
Skipjack. This is incorrect, Skipjack was developed after DES by the NSA .
Brooks-Aldeman. This is incorrect because this is a distractor, no algorithm exists with this name.

QUESTION 330
What is a characteristic of using the Electronic Code Book mode of DES encryption?

A. A given block of plaintext and a given key will always produce the same ciphertext.
B. Repetitive encryption obscures any repeated patterns that may have been present in the plaintext.
C. Individual characters are encoded by combining output from earlier encryption routines with plaintext.
D. The previous DES output is used as input.

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
A given message and key always produce the same ciphertext.

The following answers are incorrect:

Repetitive encryption obscures any repeated patterns that may have been present in the plaintext. Is incorrect because with Electronic Code Book a given 64 bit block of plaintext always produces the same ciphertext

Individual characters are encoded by combining output from earlier encryption routines with plaintext. This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached. This is a characteristic of Cipher Feedback. Cipher Feedback the ciphertext is run through a keygenerating device to create the key for the next block of plaintext.

The previous DES output is used as input. Is incorrect because This is incorrect because with Electronic Code Book processing 64 bits at a time until the end of the file was reached . This is a characteristic of Cipher Block Chaining. Cipher Block Chaining uses the output from the previous block to encrypt the next block.

QUESTION 331
Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods. What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A
Section: Cryptography
Explanation
Explanation/Reference:
A Public Key is also known as an asymmetric algorithm and the use of a secret key would be a symmetric algorithm.

The following answers are incorrect:

Use of the recipient's public key for encryption and decryption based on the recipient's private key. Is incorrect this would be known as an asymmetric algorithm. Use of software encryption assisted by a hardware encryption accelerator. This is incorrect, it is a distractor. Use of Elliptic Curve Encryption. Is incorrect this would use an asymmetric algorithm.

QUESTION 332
Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.
B. The channels through which the information flows are secure.
C. The recipient's identity can be positively verified by the sender.
D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.

The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.

The following answers are incorrect:

The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key

Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.

The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.

The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).

Reference(s) used for this question:
OIG CBK Cryptography (pages 253 - 254)

QUESTION 333
Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".

Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.

The other answers are not correct because:

"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.

"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.

"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.

Reference:
Official ISC2 Guide page: 266 (poor explanation)
All in One Third Edition page: 657 (excellent explanation)
Key Management - Page 732, All in One Fourth Edition

QUESTION 334
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The other answers are not correct because:

"Rivest, Shamir, Adleman (RSA)" is incorrect because RSA is a "traditional" asymmetric algorithm. While it is reasonably strong, it is not considered to be as strong as ECC based systems.

"El Gamal" is incorrect because it is also a "traditional" asymmetric algorithm and not considered as strong as ECC based systems.

"Advanced Encryption Standard (AES)" is incorrect because the question asks specifically about asymmetric algorithms and AES is a symmetric algorithm.

References:
Official ISC2 Guide page: 258
All in One Third Edition page: 638
The RSA Crypto FAQ: http://www.rsa.com/rsalabs/node.asp?id=2241

QUESTION 335
How many bits is the effective length of the key of the Data Encryption Standard algorithm?

A. 168

B. 128
C. 56
D. 64

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The correct answer is "56". This is actually a bit of a trick question, since the actual key length is 64 bits. However, every eighth bit is ignored because it is used for parity. This makes the "effective length of the key" that the question actually asks for 56 bits.

The other answers are not correct because:

168 - This is the number of effective bits in Triple DES (56 times 3).
128 - Many encryption algorithms use 128 bit key, but not DES. Note that you may see 128 bit encryption referred to as "military strength encryption" because many military systems use key of this length.
64 - This is the actual length of a DES encryption key, but not the "effective length" of the DES key.

Reference:
Official ISC2 Guide page: 238
All in One Third Edition page: 622

QUESTION 336
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading the password.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.

Correct Answer: B

Section: Cryptography
Explanation

Explanation/Reference:
The whole idea behind a one-way hash is that it should be just that - one-way. In other words, an attacker should not be able to figure out your password from the hashed version of that password in any mathematically feasible way (or within any reasonable length of time).

Password Hashing and Encryption

In most situations , if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure passwords are not sent in cleartext.

Although some people think the world is run by Microsoft, other types of operating systems are out there, such as Unix and Linux. These systems do not use registries and SAM databases, but contain their user passwords in a file cleverly called “shadow.” Now, this shadow file does not contain passwords in cleartext; instead, your password is run through a hashing algorithm, and the resulting value is stored in this file.

Unixtype systems zest things up by using salts in this process. Salts are random values added to the encryption process to add more complexity and randomness. The more randomness entered into the encryption process, the harder it is for the bad guy to decrypt and uncover your password. The use of a salt means that the same password can be encrypted into several thousand different formats. This makes it much more difficult for an attacker to uncover the right format for your system.

Password Cracking tools
Note that the use of one-way hashes for passwords does not prevent password crackers from guessing passwords. A password cracker runs a plain-text string through the same one-way hash algorithm used by the system to generate a hash, then compares that generated has with the one stored on the system. If they match, the password cracker has guessed your password.

This is very much the same process used to authenticate you to a system via a password. When you type your username and password, the system hashes the password you typed and compares that generated hash against the one stored on the system - if they match, you are authenticated.

Pre-Computed password tables exists today and they allow you to crack passwords on Lan Manager (LM) within a VERY short period of time through the use of Rainbow Tables. A Rainbow Table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off also called a Time-Memory trade off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack unfeasible.

You may want to review "Rainbow Tables" at the links:
http://en.wikipedia.org/wiki/Rainbow_table
http://www.antsight.com/zsl/rainbowcrack/

Today's password crackers:
Meet oclHashcat. They are GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.

This GPU cracker is a fusioned version of oclHashcat-plus and oclHashcat-lite, both very well-known suites at that time, but now deprecated. There also existed a now very old oclHashcat GPU cracker that was replaced w/ plus and lite, which - as said - were then merged into oclHashcat 1.00 again.

This cracker can crack Hashes of NTLM Version 2 up to 8 characters in less than a few hours. It is definitively a game changer. It can try hundreds of billions of tries per seconds on a very large cluster of GPU's. It supports up to 128 Video Cards at once.

I am stuck using Password what can I do to better protect myself?

You could look at safer alternative such as Bcrypt, PBKDF2, and Scrypt.

bcrypt is a key derivation function for passwords designed by Niels Provos and David Mazières, based on the Blowfish cipher, and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

In cryptography, scrypt is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the scrypt algorithm was published by the IETF as an Internet Draft, intended to become an informational RFC, which has since expired. A simplified version of scrypt is used as a proof-ofwork scheme by a number of cryptocurrencies, such as Litecoin and Dogecoin.

PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0, also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long.

PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes (rainbow tables) for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

The other answers are incorrect:

"It prevents an unauthorized person from trying multiple passwords in one logon attempt." is incorrect because the fact that a password has been hashed does not prevent this type of brute force password guessing attempt.

"It minimizes the amount of storage required for user passwords" is incorrect because hash algorithms always generate the same number of bits, regardless of the length of the input. Therefore, even short passwords will still result in a longer hash and not minimize storage requirements.

"It minimizes the amount of processing time used for encrypting passwords" is incorrect because the processing time to encrypt a password would be basically the same required to produce a one-way has of the same password.

Reference(s) used for this question:
http://en.wikipedia.org/wiki/PBKDF2
http://en.wikipedia.org/wiki/Scrypt
http://en.wikipedia.org/wiki/Bcrypt
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 195) . McGraw-Hill. Kindle Edition.

QUESTION 337
Which of the following issues is not addressed by digital signatures?

A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
A digital signature directly addresses both confidentiality and integrity of the CIA triad. It does not directly address availability, which is what denial-of-service attacks.

The other answers are not correct because:

"nonrepudiation" is not correct because a digital signature can provide for nonrepudiation.
"authentication" is not correct because a digital signature can be used as an authentication mechanism
"data integrity" is not correct because a digital signature does verify data integrity (as part of nonrepudiation)

References:
Official ISC2 Guide page: 227 & 265
All in One Third Edition page: 648

QUESTION 338
Brute force attacks against encryption keys have increased in potency because of increased computing power. Which of the following is often considered a good protection against the brute force cryptography attack?

A. The use of good key generators.
B. The use of session keys.
C. Nothing can defend you against a brute force crypto key attack.
D. Algorithms that are immune to brute force key attacks.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
If we assume a crytpo-system with a large key (and therefore a large key space) a brute force attack will likely take a good deal of time - anywhere from several hours to several years depending on a number of variables. If you use a session key for each message you encrypt, then the brute force attack provides the attacker with only the key for that one message. So, if you are encrypting 10 messages a day, each with a different session key, but it takes me a month to break each session key then I am fighting a loosing battle.

The other answers are not correct because:
"The use of good key generators" is not correct because a brute force key attack will eventually run through all possible combinations of key. Therefore, any key will eventually be broken in this manner given enough time.

"Nothing can defend you against a brute force crypto key attack" is incorrect, and not the best answer listed. While it is technically true that any key will eventually be broken by a brute force attack, the question remains "how long will it take?". In other words, if you encrypt something today but I can't read it for 10,000 years, will you still care? If the key is changed every session does it matter if it can be broken after the session has ended? Of the answers listed here, session keys are "often considered a good protection against the brute force cryptography attack" as the question asks.

"Algorithms that are immune to brute force key attacks" is incorrect because there currently are no such algorithms.

References:
Official ISC2 Guide page: 259
All in One Third Edition page: 623

QUESTION 339
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

A. 64 bits of data input results in 56 bits of encrypted output

B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so the effective key length is 56 bits).

Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64 bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS197.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.

IN CONTRAST WITH AES

The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.

The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.

The AES algorithm may be used with the three different key lengths indicated above, and therefore these different “flavors” may be referred to as “AES-128”, “AES192”, and “AES-256”.

The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with 64 bit block input, it results in 64 bit blocks of encrypted output.

"128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key.

"56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.

Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 340
PGP uses which of the following to encrypt data?

A. An asymmetric encryption algorithm
B. A symmetric encryption algorithm

C. A symmetric key distribution system
D. An X.509 digital certificate

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Notice that the question specifically asks what PGP uses to encrypt For this, PGP uses an symmetric key algorithm. PGP then uses an asymmetric key algorithm to encrypt the session key and then send it securely to the receiver. It is an hybrid system where both types of ciphers are being used for different purposes.

Whenever a question talks about the bulk of the data to be sent, Symmetric is always best to choice to use because of the inherent speed within Symmetric Ciphers. Asymmetric ciphers are 100 to 1000 times slower than Symmetric Ciphers.

The other answers are not correct because:

"An asymmetric encryption algorithm" is incorrect because PGP uses a symmetric algorithm to encrypt data.

"A symmetric key distribution system" is incorrect because PGP uses an asymmetric algorithm for the distribution of the session keys used for the bulk of the data.

"An X.509 digital certificate" is incorrect because PGP does not use X.509 digital certificates to encrypt the data, it uses a session key to encrypt the data.

References:
Official ISC2 Guide page: 275
All in One Third Edition page: 664 - 665

QUESTION 341
What is NOT true with pre shared key authentication within IKE / IPsec protocol?

A. Pre shared key authentication is normally based on simple passwords
B. Needs a Public Key Infrastructure (PKI) to work
C. IKE is used to setup Security Associations
D. IKE builds upon the Oakley protocol and the ISAKMP protocol.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication which are either pre-shared or distributed using DNS (preferably with DNSSEC) and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

Internet Key Exchange (IKE) Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and is applied as an authentication component of IPSec.

IKE uses two phases:

Phase 1: In this phase, the partners authenticate with each other, using one of the following:
Shared Secret: A key that is exchanged by humans via telephone, fax, encrypted e-mail, etc.
Public Key Encryption: Digital certificates are exchanged.
Revised mode of Public Key Encryption: To reduce the overhead of public key encryption, a nonce (a Cryptographic function that refers to a number or bit string used only once, in security engineering) is encrypted with the communicating partner's public key, and the peer's identity is encrypted with symmetric encryption using the nonce as the key. Next, IKE establishes a temporary security association and secure tunnel to protect the rest of the key exchange. Phase 2: The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7032-7048). Auerbach Publications. Kindle Edition. and
RFC 2409 at http://tools.ietf.org/html/rfc2409
and
http://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION 342
In a hierarchical PKI the highest CA is regularly called Root CA, it is also referred to by which one of the following term?

A. Subordinate CA
B. Top Level CA
C. Big CA
D. Master CA

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Reference: Arsenault, Turner, Internet X.509 Public Key Infrastructure: Roadmap, Chapter "Terminology".

Also note that sometimes other terms such as Certification Authority Anchor (CAA) might be used within some government organization, Top level CA is another common term to indicate the top level CA, Top Level Anchor could also be used.

QUESTION 343
What is the primary role of cross certification?

A. Creating trust between different PKIs
B. Build an overall PKI hierarchy
C. set up direct trust to a second root CA
D. Prevent the nullification of user certificates by CA certificate revocation

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:

More and more organizations are setting up their own internal PKIs. When these independent PKIs need to interconnect to allow for secure communication to take place (either between departments or different companies), there must be a way for the two root CAs to trust each other.

These two CAs do not have a CA above them they can both trust, so they must carry out cross certification. A cross certification is the process undertaken by CAs to establish a trust relationship in which they rely upon each other's digital certificates and public keys as if they had issued them themselves.

When this is set up, a CA for one company can validate digital certificates from the other company and vice versa.

Reference(s) used for this question:

For more information and illustration on Cross certification: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx http://www.entrust.com/resources/pdf/cross_certification.pdf

also see:
Shon Harris, CISSP All in one book, 4th Edition, Page 727
and
RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile; FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 254.

QUESTION 344
What kind of encryption is realized in the S/MIME-standard?

A. Asymmetric encryption scheme
B. Password based encryption scheme
C. Public key based, hybrid encryption scheme
D. Elliptic curve based encryption

Correct Answer: C
Section: Cryptography
Explanation
Explanation/Reference:
S/MIME (for Secure MIME, or Secure Multipurpose Mail Extension) is a security process used for e-mail exchanges that makes it possible to guarantee the confidentiality and non-repudiation of electronic messages.
S/MIME is based on the MIME standard, the goal of which is to let users attach files other than ASCII text files to electronic messages. The MIME standard therefore makes it possible to attach all types of files to e-mails.

S/MIME was originally developed by the company RSA Data Security. Ratified in July 1999 by the IETF, S/MIME has become a standard, whose specifications are contained in RFCs 2630 to 2633. How S/MIME works

The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.

The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.

The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message.

In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

Reference(s) used for this question:
http://en.kioskea.net/contents/139-cryptography-s-mime
RFC 2630: Cryptographic Message Syntax;
OPPLIGER, Rolf, Secure Messaging with PGP and S/MIME, 2000, Artech House;
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 570;
SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 345
What is the main problem of the renewal of a root CA certificate?

A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate

Correct Answer: B
Section: Cryptography
Explanation
Explanation/Reference:
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).

In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.

Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).

The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.

Reference: Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION 346
Virus scanning and content inspection of SMIME encrypted e-mail without doing any further processing is:

A. Not possible
B. Only possible with key recovery scheme of all user keys
C. It is possible only if X509 Version 3 certificates are used
D. It is possible only by "brute force" decryption

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Content security measures presumes that the content is available in cleartext on the central mail server.

Encrypted emails have to be decrypted before it can be filtered (e.g. to detect viruses), so you need the decryption key on the central "crypto mail server".

There are several ways for such key management, e.g. by message or key recovery methods. However, that would certainly require further processing in order to achieve such goal.

QUESTION 347
What attribute is included in a X.509-certificate?

A. Distinguished name of the subject
B. Telephone number of the department
C. secret key of the issuing CA
D. the key pair of the certificate holder

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 348
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 139;

SNYDER, J., What is a SMART CARD?.
Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance
Security

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.

Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.

It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:

physical attack of various forms (microprobing, drills, files, solvents, etc.)
freezing the device
applying out-of-spec voltages or power
surges applying unusual clock signals
inducing software errors using radiation
measuring the precise time and power
requirements of certain operations (see power
analysis)

Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.

Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 349
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.

Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.

A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.

In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers.

Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.

References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 350
What does the directive of the European Union on Electronic Signatures deal with?

A. Encryption of classified data
B. Encryption of secret data
C. Non repudiation
D. Authentication of web servers

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Reference: FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 589; Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures.

QUESTION 351
A X.509 public key certificate with the key usage attribute "non repudiation" can be used for which of the following?

A. encrypting messages

B. signing messages
C. verifying signed messages
D. decrypt encrypted messages

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
References: RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide.

QUESTION 352
Which of the following would best describe certificate path validation?

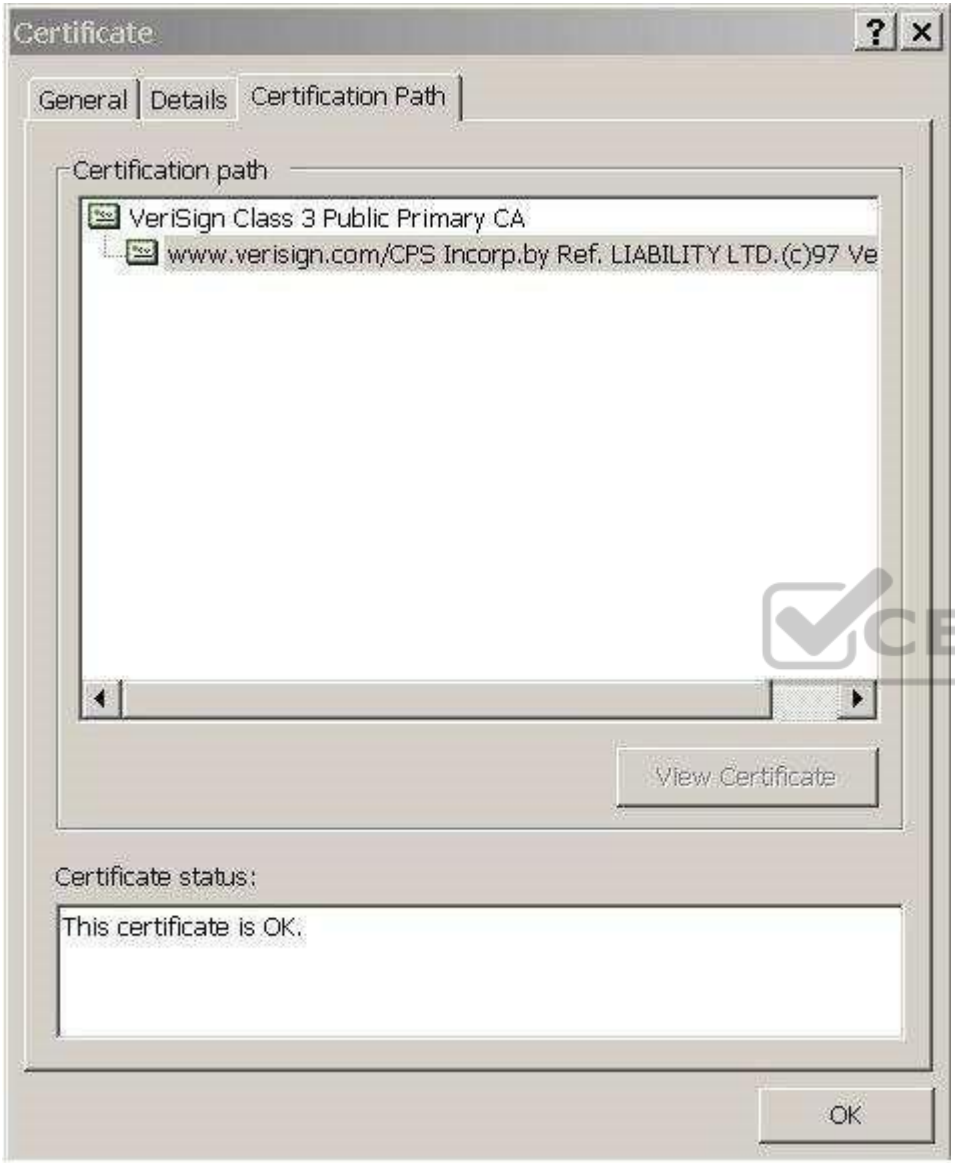
A. Verification of the validity of all certificates of the certificate chain to the root certificate
B. Verification of the integrity of the associated root certificate
C. Verification of the integrity of the concerned private key
D. Verification of the revocation status of the concerned certificate

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
With the advent of public key cryptography (PKI), it is now possible to communicate securely with untrusted parties over the Internet without prior arrangement. One of the necessities arising from such communication is the ability to accurately verify someone's identity (i.e. whether the person you are communicating with is indeed the person who he/she claims to be). In order to be able to perform identity check for a given entity, there should be a fool-proof method of “binding” the entity's public key to its unique domain name (DN).

A X.509 digital certificate issued by a well known certificate authority (CA), like Verisign, Entrust, Thawte, etc., provides a way of positively identifying the entity by placing trust on the CA to have performed the necessary verifications. A X.509 certificate is a cryptographically sealed data object that contains the entity's unique DN, public key, serial number, validity period, and possibly other extensions.

The Windows Operating System offers a Certificate Viewer utility which allows you to double-click on any certificate and review its attributes in a human-readable format. For instance, the "General" tab in the Certificate Viewer Window (see below) shows who the certificate was issued to as well as the certificate's issuer, validation period and usage functions.



Certification Path graphic

The “Certification Path” tab contains the hierarchy for the chain of certificates. It allows you to select the certificate issuer or a subordinate certificate and then click on “View Certificate” to open the certificate in the Certificate Viewer.

Each end-user certificate is signed by its issuer, a trusted CA, by taking a hash value (MD5 or SHA-1) of ASN.1 DER (Distinguished Encoding Rule) encoded object and then encrypting the resulting hash with the issuer’s private key (CA's Private Key) which is a digital signature. The encrypted data is stored in the “signatureValue” attribute of the entity’s (CA) public certificate.

Once the certificate is signed by the issuer, a party who wishes to communicate with this entity can then take the entity’s public certificate and find out who the issuer of the certificate is. Once the issuer’s of the certificate (CA) is identified, it would be possible to decrypt the value of the “signatureValue” attribute in the entity's certificate using the issuer’s public key to retrieve the hash value. This hash value will be compared with the independently calculated hash on the entity's certificate. If the two hash values match, then the information contained within the certificate must not have been altered and, therefore, one must trust that the CA has done enough background check to ensure that all details in the entity’s certificate are accurate.

The process of cryptographically checking the signatures of all certificates in the certificate chain is called “key chaining”. An additional check that is essential to key chaining is verifying that the value of the "subjectKeyIdentifier” extension in one certificate matches the same in the subsequent certificate.

Similarly, the process of comparing the subject field of the issuer certificate to the issuer field of the subordinate certificate is called “name chaining”. In this process, these values must match for each pair of adjacent certificates in the certification path in order to guarantee that the path represents unbroken chain of entities relating directly to one another and that it has no missing links.

The two steps above are the steps to validate the Certification Path by ensuring the validity of all certificates of the certificate chain to the root certificate as described in the two paragraphs above.

Reference(s) used for this question:
FORD, Warwick & BAUM, Michael S., Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption (2nd Edition), 2000, Prentice Hall PTR, Page 262.
and https://www.tibcommunity.com/docs/DOC-2197

QUESTION 353
Which of the following can best define the "revocation request grace period"?

A. The period of time allotted within which the user must make a revocation request upon a revocation reason
B. Minimum response time for performing a revocation by the CA
C. Maximum response time for performing a revocation by the CA
D. Time period between the arrival of a revocation request and the publication of the revocation information

Correct Answer: D

Section: Cryptography
Explanation

Explanation/Reference:
The length of time between the Issuer's receipt of a revocation request and the time the Issuer is required to revoke the certificate should bear a reasonable relationship to the amount of risk the participants are willing to assume that someone may rely on a certificate for which a proper evocation request has been given but has not yet been acted upon.

How quickly revocation requests need to be processed (and CRLs or certificate status databases need to be updated) depends upon the specific application for which the Policy Authority is rafting the Certificate Policy.

A Policy Authority should recognize that there may be risk and lost tradeoffs with respect to grace periods for revocation notices.
If the Policy Authority determines that its PKI participants are willing to accept a grace period of a few hours in exchange for a lower implementation cost, the Certificate Policy may reflect that decision.

QUESTION 354
Which is NOT a suitable method for distributing certificate revocation information?

A. CA revocation mailing list
B. Delta CRL
C. OCSP (online certificate status protocol)
D. Distribution point CRL

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
The following are incorrect answers because they are all suitable methods.

A Delta CRL is a CRL that only provides information about certificates whose statuses have changed since the issuance of a specific, previously issued CRL.

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

A Distribution point CRL or CRL Distribution Point, a location specified in the CRL Distribution Point (CRL DP) X.509, version 3, certificate extension when the certificate is issued.

References:

RFC 2459: Internet X.509 Public Key Infrastru
http://csrc.nist.gov/groups/ST/crypto_apps_infra/documents/sliding_window.pdf
http://www.ipswitch.eu/online_certificate_status_protocol_en.html
Computer Security Handbook By Seymour Bosworth, Arthur E. Hutt, Michel E. Kabay http://books.google.com/books?id=rCx5OfSFUPkC&printsec=frontcover&dq=Computer+Security+Handbook#PRA6-PA4,M1

QUESTION 355
Which of the following is true about digital certificate?

A. It is the same as digital signature proving Integrity and Authenticity of the data
B. Electronic credential proving that the person the certificate was issued to is who they claim to be
C. You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.
D. Can't contain geography data such as country for example.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Digital certificate helps others verify that the public keys presented by users are genuine and valid. It is a form of Electronic credential proving that the person the certificate was issued to is who they claim to be.

The certificate is used to identify the certificate holder when conducting electronic transactions.
It is issued by a certification authority (CA). It contains the name of an organization or individual, the business address, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

Digital certificates are key to the PKI process. The digital certificate serves two roles. First, it ensures the integrity of the public key and makes sure that the key remains unchanged and in a valid state. Second, it validates that the public key is tied to the stated owner and that all associated information is true and correct. The information needed to accomplish these goals is added into the digital certificate.

A Certificate Authority (CA) is an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates.
A Registration Authority (RA) performs certificate registration services on behalf of a CA. The RA, a single purpose server, is responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate request.

A Digital Certificate is not like same as a digital signature, they are two different things, a digital Signature is created by using your Private key to encrypt a message digest and a Digital Certificate is issued by a trusted third party who vouch for your identity.

There are many other third parties which are providing Digital Certifictes and not just Verisign, RSA.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 14894-14903). Auerbach Publications. Kindle Edition.

Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware: Exam CAS-001 (p. 24). Wiley. Kindle Edition.

Please refer to http://en.wikipedia.org/wiki/Digital_certificate
What is Digital certificate: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211947,00.html
another deifination on http://www.webopedia.com/TERM/D/digital_certificate.html

QUESTION 356
What kind of Encryption technology does SSL utilize?

A. Secret or Symmetric key
B. Hybrid (both Symmetric and Asymmetric)
C. Public Key
D. Private key

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
SSL use public-key cryptography to secure session key, while the session key (secret key) is used to secure the whole session taking place between both parties communicating with each other.

The SSL protocol was originally developed by Netscape. Version 1.0 was never publicly released; version 2.0 was released in February 1995 but "contained a number of security flaws which ultimately led to the design of SSL version 3.0." SSL version 3.0, released in 1996, was a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier. All of the other answers are incorrect

QUESTION 357
What is the name of a one way transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string? Such a transformation cannot be reversed?

A. One-way hash
B. DES

C. Transposition
D. Substitution

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
A cryptographic hash function is a transformation that takes an input (or 'message') and returns a fixed-size string, which is called the hash value (sometimes termed a message digest, a digital fingerprint, a digest or a checksum).

The ideal hash function has three main properties - it is extremely easy to calculate a hash for any given data, it is extremely difficult or almost impossible in a practical sense to calculate a text that has a given hash, and it is extremely unlikely that two different messages, however close, will have the same hash.

Functions with these properties are used as hash functions for a variety of purposes, both within and outside cryptography. Practical applications include message integrity checks, digital signatures, authentication, and various information security applications. A hash can also act as a concise representation of the message or document from which it was computed, and allows easy indexing of duplicate or unique data files.

In various standards and applications, the two most commonly used hash functions are MD5 and SHA-1. In 2005, security flaws were identified in both of these, namely that a possible mathematical weakness might exist, indicating that a stronger hash function would be desirable. In 2007 the National Institute of Standards and Technology announced a contest to design a hash function which will be given the name SHA-3 and be the subject of a FIPS standard.

A hash function takes a string of any length as input and produces a fixed length string which acts as a kind of "signature" for the data provided. In this way, a person knowing the hash is unable to work out the original message, but someone knowing the original message can prove the hash is created from that message, and none other. A cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable.

A cryptographic hash function is considered "insecure" from a cryptographic point of view, if either of the following is computationally feasible:

finding a (previously unseen) message that matches a given digest finding "collisions", wherein two different messages have the same message digest.

An attacker who can do either of these things might, for example, use them to substitute an authorized message with an unauthorized one.

Ideally, it should not even be feasible to find two messages whose digests are substantially similar; nor would one want an attacker to be able to learn anything useful about a message given only its digest. Of course the attacker learns at least one piece of information, the digest itself, which for instance gives the attacker the ability to recognise the same message should it occur again.

REFERENCES:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Pages 4041. also see: http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 358
Which of the following is NOT an asymmetric key algorithm?

A. RSA
B. Elliptic Curve Cryptosystem (ECC)
C. El Gamal
D. Data Encryption System (DES)

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the key size was reduced to 56 bits, plus 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST. All other options are asymmetric algorithms.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 525).
Reference: DES: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 359
Which of the following is NOT a symmetric key algorithm?

A. Blowfish
B. Digital Signature Standard (DSS)
C. Triple DES (3DES)
D. RC5

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:

Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital signature, providing the capability to generate signatures (with the use of a private key) and verify them (with the use of the corresponding public key).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 550).
Reference: DSS: http://www.itl.nist.gov/fipspubs/fip186.htm.

QUESTION 360
Which of the following ASYMMETRIC encryption algorithms is based on the difficulty of FACTORING LARGE NUMBERS?

A. El Gamal
B. Elliptic Curve Cryptosystems (ECCs)
C. RSA
D. International Data Encryption Algorithm (IDEA)

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Named after its inventors Ron Rivest , Adi Shamir and Leonard Adleman is based on the difficulty of factoring large prime numbers.

Factoring a number means representing it as the product of prime numbers. Prime numbers, such as 2, 3, 5, 7, 11, and 13, are those numbers that are not evenly divisible by any smaller number, except 1. A non-prime, or composite number, can be written as the product of smaller primes, known as its prime factors. 665, for example is the product of the primes 5, 7, and 19. A number is said to be factored when all of its prime factors are identified. As the size of the number increases, the difficulty of factoring increases rapidly.

The other answers are incorrect because:

El Gamal is based on the discrete logarithms in a finite field.
Elliptic Curve Cryptosystems (ECCs) computes discrete logarithms of elliptic curves.
International Data Encryption Algorithm (IDEA) is a block cipher and operates on 64 bit blocks of data and is a SYMMETRIC algorithm.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 638

QUESTION 361
The Diffie-Hellman algorithm is primarily used to provide which of the following?

A. Confidentiality
B. Key Agreement

C. Integrity
D. Non-repudiation

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Diffie and Hellman describe a means for two parties to agree upon a shared secret in such a way that the secret will be unavailable to eavesdroppers. This secret may then be converted into cryptographic keying material for other (symmetric) algorithms. A large number of minor variants of this process exist. See RFC 2631 Diffie-Hellman Key Agreement Method for more details.

In 1976, Diffie and Hellman were the first to introduce the notion of public key cryptography, requiring a system allowing the exchange of secret keys over nonsecure channels. The Diffie-Hellman algorithm is used for key exchange between two parties communicating with each other, it cannot be used for encrypting and decrypting messages, or digital signature.
Diffie and Hellman sought to address the issue of having to exchange keys via courier and other unsecure means. Their efforts were the FIRST asymmetric key agreement algorithm. Since the Diffie-Hellman algorithm cannot be used for encrypting and decrypting it cannot provide confidentiality nor integrity. This algorithm also does not provide for digital signature functionality and thus non-repudiation is not a choice.

NOTE: The DH algorithm is susceptible to man-in-the-middle attacks.

KEY AGREEMENT VERSUS KEY EXCHANGE
A key exchange can be done multiple way. It can be done in person, I can generate a key and then encrypt the key to get it securely to you by encrypting it with your public key. A Key Agreement protocol is done over a public medium such as the internet using a mathematical formula to come out with a common value on both sides of the communication link, without the ennemy being able to know what the common agreement is.

The following answers were incorrect:

All of the other choices were not correct choices

Reference(s) used for this question:
Shon Harris, CISSP All In One (AIO), 6th edition . Chapter 7, Cryptography, Page 812.
http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
http://www.google.com/patents?vid=4200770

QUESTION 362
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.

The following answers are incorrect because :

SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.
S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.
SSL is incorrect as it uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication.

Reference : Shon Harris AIO v3 , Chapter-8: Cryptography , Page : 667-669

QUESTION 363
Which of the following algorithms does NOT provide hashing?

A. SHA-1
B. MD2

C. RC4
D. MD5

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
As it is an algorithm used for encryption and does not provide hashing functions , it is also commonly implemented ' Stream Ciphers '.

The other answers are incorrect because :
SHA-1 was designed by NIST and NSA to be used with the Digital Signature Standard (DSS). SHA was designed to be used in digital signatures and was developed when a more secure hashing algorithm was required for U.S. government applications.

MD2 is a one-way hash function designed by Ron Rivest that creates a 128-bit message digest value. It is not necessarily any weaker than the other algorithms in the "MD" family, but it is much slower.

MD5 was also created by Ron Rivest and is the newer version of MD4. It still produces a 128-bit hash, but the algorithm is more complex, which makes it harder to break.

Reference : Shon Harris , AIO v3 , Chapter - 8 : Cryptography , Page : 644 - 645

QUESTION 364
In what type of attack does an attacker try, from several encrypted messages, to figure out the key used in the encryption process?

A. Known-plaintext attack
B. Ciphertext-only attack
C. Chosen-Ciphertext attack
D. Plaintext-only attack

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
In a ciphertext-only attack, the attacker has the ciphertext of several messages encrypted with the same encryption algorithm. Its goal is to discover the plaintext of the messages by figuring out the key used in the encryption process. In a known-plaintext attack, the attacker has the plaintext and the ciphertext of one or more messages. In a chosen-ciphertext attack, the attacker can chose the ciphertext to be decrypted and has access to the resulting plaintext.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 8: Cryptography (page 578).

QUESTION 365
Which encryption algorithm is BEST suited for communication with handheld wireless devices?

A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution,and encryption. One differing factor is ECC's efficiency. ECC is more efficient that RSA and any other asymmetric algorithm.

The following answers are incorrect because :

RSA is incorrect as it is less efficient than ECC to be used in handheld devices.
SHA is also incorrect as it is a hashing algorithm.
RC4 is also incorrect as it is a symmetric algorithm.
Reference : Shon Harris AIO v3 , Chapter-8 : Cryptography , Page : 631 , 638.

QUESTION 366
Which of the following keys has the SHORTEST lifespan?

A. Secret key
B. Public key
C. Session key
D. Private key

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:

As session key is a symmetric key that is used to encrypt messages between two users. A session key is only good for one communication session between users.

For example , If Tanya has a symmetric key that she uses to encrypt messages between Lance and herself all the time , then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However , using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If , on the other hand , a new symmetric key were generated each time Lance and Tanya wanted to communicate , it would be used only during their dialog and then destroyed. if they wanted to communicate and hour later , a new session key would be created and shared.

The other answers are not correct because :

Public Key can be known to anyone.
Private Key must be known and used only by the owner.
Secret Keys are also called as Symmetric Keys, because this type of encryption relies on each user to keep the key a secret and properly protected.

REFERENCES:
SHON HARRIS , ALL IN ONE THIRD EDITION : Chapter 8 : Cryptography , Page : 619-620

QUESTION 367
What is the RESULT of a hash algorithm being applied to a message ?

A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
As when a hash algorithm is applied on a message , it produces a message digest.

The other answers are incorrect because :

A digital signature is a hash value that has been encrypted with a sender's private key.
A ciphertext is a message that appears to be unreadable.

A plaintext is a readable data.
Reference : Shon Harris , AIO v3 , Chapter-8 : Cryptography , Page : 593-594 , 640 , 648

QUESTION 368
Secure Sockets Layer (SSL) uses a Message Authentication Code (MAC) for what purpose?

A. message non-repudiation.
B. message confidentiality.
C. message interleave checking.
D. message integrity.

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
A keyed hash also called a MAC (message authentication code) is used for integrity protection and authenticity.

In cryptography, a message authentication code (MAC) is a generated value used to authenticate a message. A MAC can be generated by HMAC or CBC-MAC methods. The MAC protects both a message's integrity (by ensuring that a different MAC will be produced if the message has changed) as well as its authenticity, because only someone who knows the secret key could have modified the message.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.

HMAC
When using HMAC the symmetric key of the sender would be concatenated (added at the end) with the message. The result of this process (message + secret key) would be put through a hashing algorithm, and the result would be a MAC value. This MAC value is then appended to the message being sent. If an enemy were to intercept this message and modify it, he would not have the necessary symmetric key to create a valid MAC value. The receiver would detect the tampering because the MAC value would not be valid on the receiving side.

CBC-MAC
If a CBC-MAC is being used, the message is encrypted with a symmetric block cipher in CBC mode, and the output of the final block of ciphertext is used as the MAC. The sender does not send the encrypted version of the message, but instead sends the plaintext version and the MAC attached to the message. The receiver receives the plaintext message and encrypts it with the same symmetric block cipher in CBC mode and calculates an independent MAC value. The receiver compares the new MAC value with the MAC value sent with the message. This method does not use a hashing algorithm as does HMAC.

Cipher-Based Message Authentication Code (CMAC)

Some security issues with CBC-MAC were found and they created Cipher-Based Message Authentication Code (CMAC) as a replacement. CMAC provides the same type of data origin authentication and integrity as CBC-MAC, but is more secure mathematically. CMAC is a variation of CBC-MAC. It is approved to work with AES and Triple DES. HMAC, CBC-MAC, and CMAC work higher in the network stack and can identify not only transmission errors (accidental), but also more nefarious modifications, as in an attacker messing with a message for her own benefit. This means all of these technologies can identify intentional, unauthorized modifications and accidental changes— three in one.

The following are all incorrect answers:

"Message non-repudiation" is incorrect.
Nonrepudiation is the assurance that someone cannot deny something. Typically, nonrepudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.

To repudiate means to deny. For many years, authorities have sought to make repudiation impossible in some situations. You might send registered mail, for example, so the recipient cannot deny that a letter was delivered. Similarly, a legal document typically requires witnesses to signing so that the person who signs cannot deny having done so.

On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

"Message confidentiality" is incorrect. The Message confidentiality is protected by encryption not by hashing algorithms.

"Message interleave checking" is incorrect. This is a nonsense term included as a distractor.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 1384). McGraw-Hill. Kindle Edition.
and
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf
and
http://searchsecurity.techtarget.com/definition/nonrepudiation
and
https://en.wikipedia.org/wiki/Message_authentication_code

QUESTION 369
Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption
B. Integrity
C. Digital signatureD. Authentication

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

QUESTION 370
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Key clustering happens when a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 130).

QUESTION 371
Which of the following is true about link encryption?

A. Each entity has a common key with the destination node.

B. Encrypted messages are only decrypted by the final node.
C. This mode does not provide protection if anyone of the nodes along the transmission path is compromised.
D. Only secure nodes are used in this type of transmission.

Correct Answer: C

Section: Cryptography
Explanation

Explanation/Reference:
In link encryption, each entity has keys in common with its two neighboring nodes in the transmission chain.

Thus, a node receives the encrypted message from its predecessor, decrypts it, and then re-encrypts it with a new key, common to the successor node. Obviously, this mode does not provide protection if anyone of the nodes along the transmission path is compromised.

Encryption can be performed at different communication levels, each with different types of protection and implications. Two general modes of encryption implementation are link encryption and end-to-end encryption.

Link encryption encrypts all the data along a specific communication path, as in a satellite link, T3 line, or telephone circuit. Not only is the user information encrypted, but the header, trailers, addresses, and routing data that are part of the packets are also encrypted. The only traffic not encrypted in this technology is the data link control messaging information, which includes instructions and parameters that the different link devices use to synchronize communication methods. Link encryption provides protection against packet sniffers and eavesdroppers.

In end-to-end encryption, the headers, addresses, routing, and trailer information are not encrypted, enabling attackers to learn more about a captured packet and where it is headed.

Reference(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 845-846). McGraw-Hill.
And:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 132).

QUESTION 372
What uses a key of the same length as the message where each bit or character from the plaintext is encrypted by a modular addition?

A. Running key cipher
B. One-time pad
C. Steganography
D. Cipher block chaining

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:

In cryptography, the one-time pad (OTP) is a type of encryption that is impossible to crack if used correctly. Each bit or character from the plaintext is encrypted by a modular addition with a bit or character from a secret random key (or pad) of the same length as the plaintext, resulting in a ciphertext. If the key is truly random, at least as long as the plaintext, never reused in whole or part, and kept secret, the ciphertext will be impossible to decrypt or break without knowing the key. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used.

First described by Frank Miller in 1882, the one-time pad was re-invented in 1917 and patented a couple of years later. It is derived from the Vernam cipher, named after Gilbert Vernam, one of its inventors. Vernam's system was a cipher that combined a message with a key read from a punched tape. In its original form, Vernam's system was vulnerable because the key tape was a loop, which was reused whenever the loop made a full cycle. One-time use came a little later when Joseph Mauborgne recognized that if the key tape were totally random, cryptanalysis would be impossible.

The "pad" part of the name comes from early implementations where the key material was distributed as a pad of paper, so the top sheet could be easily torn off and destroyed after use. For easy concealment, the pad was sometimes reduced to such a small size that a powerful magnifying glass was required to use it. Photos show captured KGB pads that fit in the palm of one's hand, or in a walnut shell. To increase security, one-time pads were sometimes printed onto sheets of highly flammable nitrocellulose so they could be quickly burned.

The following are incorrect answers:

A running key cipher uses articles in the physical world rather than an electronic algorithm. In classical cryptography, the running key cipher is a type of polyalphabetic substitution cipher in which a text, typically from a book, is used to provide a very long keystream. Usually, the book to be used would be agreed ahead of time, while the passage to use would be chosen randomly for each message and secretly indicated somewhere in the message.

The Running Key cipher has the same internal workings as the Vigenere cipher. The difference lies in how the key is chosen; the Vigenere cipher uses a short key that repeats, whereas the running key cipher uses a long key such as an excerpt from a book. This means the key does not repeat, making cryptanalysis more difficult. The cipher can still be broken though, as there are statistical patterns in both the key and the plaintext which can be exploited.

Steganography is a method where the very existence of the message is concealed. It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. it is sometimes referred to as Hiding in Plain Sight.

Cipher block chaining is a DES operating mode. IBM invented the cipher-block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.

Reference(s) used for this question:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 555).
and
http://en.wikipedia.org/wiki/One-time_pad
http://en.wikipedia.org/wiki/Running_key_cipher
http://en.wikipedia.org/wiki/Cipher_block_chaining#Cipher-block_chaining_.28CBC.29

QUESTION 373
What can be defined as secret communications where the very existence of the message is hidden?

A. Clustering
B. Steganography
C. Cryptology
D. Vernam cipher

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Steganography is a secret communication where the very existence of the message is hidden. For example, in a digital image, the least significant bit of each word can be used to comprise a message without causing any significant change in the image. Key clustering is a situation in which a plaintext message generates identical ciphertext messages using the same transformation algorithm but with different keys. Cryptology encompasses cryptography and cryptanalysis. The Vernam Cipher, also called a one-time pad, is an encryption scheme using a random key of the same size as the message and is used only once. It is said to be unbreakable, even with infinite resources.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 134).

QUESTION 374
Which of the following is not an example of a block cipher?

A. Skipjack B.
IDEA
C. Blowfish
D. RC4

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
RC4 is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc. Skipjack, IDEA and Blowfish are examples of block ciphers.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 375
The Diffie-Hellman algorithm is used for:

A. Encryption
B. Digital signature
C. Key agreement
D. Non-repudiation

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The Diffie-Hellman algorithm is used for Key agreement (key distribution) and cannot be used to encrypt and decrypt messages.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 4).

Note: key agreement, is different from key exchange, the functionality used by the other asymmetric algorithms.

References:
AIO, third edition Cryptography (Page 632)
AIO, fourth edition Cryptography (Page 709)

QUESTION 376
A one-way hash provides which of the following?

A. Confidentiality
B. Availability
C. Integrity
D. Authentication

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
A one-way hash is a function that takes a variable-length string a message, and compresses and transforms it into a fixed length value referred to as a hash value.
It provides integrity, but no confidentiality, availability or authentication.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 5).

QUESTION 377
Which of the following is not a one-way hashing algorithm?

A. MD2
B. RC4
C. SHA-1
D. HAVAL

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6).

RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.

The main factors in RC4's success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.

The following answer were not correct choices:
SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm".

The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA-1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA-1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved

alternatives. A new hash standard, SHA-3, is currently under development — an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.

Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.

The following reference(s) were used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
https://en.wikipedia.org/wiki/HAVAL
and
https://en.wikipedia.org/wiki/MD2_%28cryptography%29
and
https://en.wikipedia.org/wiki/SHA-1

QUESTION 378
Which of the following statements pertaining to key management is incorrect?

A. The more a key is used, the shorter its lifetime should be.
B. When not using the full keyspace, the key should be extremely random.
C. Keys should be backed up or escrowed in case of emergencies.
D. A key's lifetime should correspond with the sensitivity of the data it is protecting.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
A key should always be using the full spectrum of the keyspace and be extremely random. Other statements are correct.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 379
Which of the following statements pertaining to link encryption is false?

A. It encrypts all the data along a specific communication path.

B. It provides protection against packet sniffers and eavesdroppers.
C. Information stays encrypted from one end of its journey to the other.
D. User information, header, trailers, addresses and routing data that are part of the packets are encrypted.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
When using link encryption, packets have to be decrypted at each hop and encrypted again.

Information staying encrypted from one end of its journey to the other is a characteristic of end-to-end encryption, not link encryption.
Link Encryption vs. End-to-End Encryption

Link encryption encrypts the entire packet, including headers and trailers, and has to be decrypted at each hop.

End-to-end encryption does not encrypt the IP Protocol headers, and therefore does not need to be decrypted at each hop.

Reference: All in one, Page 735 & Glossary
and
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 6).

QUESTION 380
Cryptography does not concern itself with which of the following choices?

A. Availability
B. Integrity
C. Confidentiality
D. Validation

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity. Unlike the other domains, cryptography does not completely support the standard of availability.

Availability
Cryptography supports all three of the core principles of information security. Many access control systems use cryptography to limit access to systems through the use of passwords. Many token-based authentication systems use cryptographic-based hash algorithms to compute one-time passwords. Denying unauthorized access prevents an attacker from entering and damaging the system or network, thereby denying access to authorized users if they damage or currupt the data.

Confidentiality
Cryptography provides confidentiality through altering or hiding a message so that ideally it cannot be understood by anyone except the intended recipient.

Integrity
Cryptographic tools provide integrity checks that allow a recipient to verify that a message has not been altered. Cryptographic tools cannot prevent a message from being altered, but they are effective to detect either intentional or accidental modification of the message.
Additional Features of Cryptographic Systems In addition to the three core principles of information security listed above, cryptographic tools provide several more benefits.

Nonrepudiation
In a trusted environment, the authentication of the origin can be provided through the simple control of the keys. The receiver has a level of assurance that the message was encrypted by the sender, and the sender has trust that the message was not altered once it was received. However, in a more stringent, less trustworthy environment, it may be necessary to provide assurance via a third party of who sent a message and that the message was indeed delivered to the right recipient. This is accomplished through the use of digital signatures and public key encryption. The use of these tools provides a level of nonrepudiation of origin that can be verified by a third party.

Once a message has been received, what is to prevent the recipient from changing the message and contesting that the altered message was the one sent by the sender? The nonrepudiation of delivery prevents a recipient from changing the message and falsely claiming that the message is in its original state. This is also accomplished through the use of public key cryptography and digital signatures and is verifiable by a trusted third party.

Authentication
Authentication is the ability to determine if someone or something is what it declares to be. This is primarily done through the control of the keys, because only those with access to the key are able to encrypt a message. This is not as strong as the nonrepudiation of origin, which will be reviewed shortly Cryptographic functions use several methods to ensure that a message has not been changed or altered. These include hash functions, digital signatures, and message authentication codes (MACs). The main concept is that the recipient is able to detect any change that has been made to a message, whether accidentally or intentionally.

Access Control
Through the use of cryptographic tools, many forms of access control are supported—from log-ins via passwords and passphrases to the prevention of access to confidential files or messages. In all cases, access would only be possible for those individuals that had access to the correct cryptographic keys.

NOTE FROM CLEMENT:
As you have seen this question was very recently updated with the latest content of the Official ISC2 Guide (OIG) to the CISSP CBK, Version 3.

Myself, I agree with most of you that cryptography does not help on the availability side and it is even the contrary sometimes if you loose the key for example. In such case you would loose access to the data and negatively impact availability. But the ISC2 is not about what I think or what you think, they have their own view of the world where they claim and state clearly that cryptography does address availability even thou it does not fully address it.

They look at crypto as the ever emcompassing tool it has become today. Where it can be use for authentication purpose for example where it would help to avoid corruption of the data through illegal access by an unauthorized user.

The question is worded this way in purpose, it is VERY specific to the CISSP exam context where ISC2 preaches that cryptography address availability even thou they state it does not fully address it. This is something new in the last edition of their book and something you must be aware of.

Best regards
Clement

The following terms are from the Software Development Security domain:

Validation: The assurance that a product, service, or system meets the needs of the customer and other identified stakeholders. It often involves acceptance and suitability with external customers. Contrast with verification below."

Verification: The evaluation of whether or not a product, service, or system complies with a regulation, requirement, specification, or imposed condition. It is often an internal process. Contrast with validation."

The terms above are from the Software Development Security Domain.

Reference(s) used for this question:
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 227-244). . Kindle Edition.
and
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Cryptography (Kindle Locations 206-227). . Kindle Edition.
and
http://en.wikipedia.org/wiki/Verification_and_validation

QUESTION 381
Which of the following does NOT concern itself with key management?

A. Internet Security Association Key Management Protocol (ISAKMP)
B. Diffie-Hellman (DH)
C. Cryptology (CRYPTO)

D. Key Exchange Algorithm (KEA)

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Cryptology is the science that includes both cryptography and cryptanalysis and is not directly concerned with key management. Cryptology is the mathematics, such as number theory, and the application of formulas and algorithms, that underpin cryptography and cryptanalysis.

The following are all concerned with Key Management which makes them the wrong choices:

Internet Security Association Key Management Protocol (ISAKMP) is a key management protocol used by IPSec. ISAKMP (Internet Security Association and Key Management Protocol) is a protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange. The actual key exchange is done by the Oakley Key Determination Protocol which is a keyagreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie-Hellman key exchange algorithm.

Diffie-Hellman and one variation of the Diffie-Hellman algorithm called the Key Exchange Algorithm (KEA) are also key exchange protocols. Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Diffie–Hellman key exchange (D–H) is a specific method of exchanging keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Reference(s) used for this question:
Mike Meyers CISSP Certification Passport, by Shon Harris and Mike Meyers, page 228.
It is highlighted as an EXAM TIP. Which tells you that it is a must know for the purpose of the exam.
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, Fifth Edition, Chapter 8: Cryptography (page 713-715).
and
https://en.wikipedia.org/wiki/ISAKMP
and
http://searchsecurity.techtarget.com/definition/cryptology

QUESTION 382
Which of the following encryption algorithms does not deal with discrete logarithms?

A. El Gamal
B. Diffie-Hellman

C. RSA
D. Elliptic Curve

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult

Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 159).
Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

QUESTION 383
Which of the following statements pertaining to message digests is incorrect?

A. The original file cannot be created from the message digest.
B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Messages digests are usually of fixed size.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 160).

QUESTION 384
Which type of attack is based on the probability of two different messages using the same hash function producing a common message digest?

A. Differential cryptanalysis
B. Differential linear cryptanalysis
C. Birthday attack
D. Statistical attack

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
A Birthday attack is usually applied to the probability of two different messages using the same hash function producing a common message digest.

The term "birthday" comes from the fact that in a room with 23 people, the probability of two of more people having the same birthday is greater than 50%.

Linear cryptanalysis is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Differential Cryptanalysis is a potent cryptanalytic technique introduced by Biham and Shamir. Differential cryptanalysis is designed for the study and attack of DESlike cryptosystems. A DES-like cryptosystem is an iterated cryptosystem which relies on conventional cryptographic techniques such as substitution and diffusion.

Differential cryptanalysis is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in an input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformations, discovering where the cipher exhibits non-random behaviour, and exploiting such properties to recover the secret key. Source:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 163).
and
http://en.wikipedia.org/wiki/Differential_cryptanalysis

QUESTION 385
Which of the following elements is NOT included in a Public Key Infrastructure (PKI)?

A. Timestamping
B. Repository
C. Certificate revocation
D. Internet Key Exchange (IKE)

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:

Other elements are included in a PKI.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 165).

QUESTION 386
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
In order to protect against fraud in electronic fund transfers (EFT), the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC).

The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.

The Secure Electronic Transaction (SET) was developed by a consortium including MasterCard and VISA as a means of preventing fraud from occurring during electronic payment.

The Secure Hash Standard (SHS), NIST FIPS 180, available at http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).

Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170)

also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html and
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

QUESTION 387
Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.

The following reference(s) were used for this question:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 170).

QUESTION 388
What is the name of the protocol use to set up and manage Security Associations (SA) for IP Security (IPSec)?

A. Internet Key Exchange (IKE)
B. Secure Key Exchange Mechanism
C. Oakley
D. Internet Security Association and Key Management Protocol

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
The Key management for IPSec is called the Internet Key Exchange (IKE)

Note: IKE underwent a series of improvements establishing IKEv2 with RFC 4306. The basis of this answer is IKEv2.

The IKE protocol is a hybrid of three other protocols: ISAKMP (Internet Security Association and Key Management Protocol), Oakley and SKEME. ISAKMP provides a framework for authentication and key exchange, but does not define them (neither authentication nor key exchange). The Oakley protocol describes a series of modes for key exchange and the SKEME protocol defines key exchange techniques.

IKE—Internet Key Exchange. A hybrid protocol that implements Oakley and Skeme key exchanges inside the ISAKMP framework. IKE can be used with other protocols, but its initial implementation is with the IPSec protocol. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.
IKE is implemented in accordance with RFC 2409, The Internet Key Exchange.

The Internet Key Exchange (IKE) security protocol is a key management protocol standard that is used in conjunction with the IPSec standard. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.
IKE is a hybrid protocol that implements the Oakley key exchange and the SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols implemented by IKE.)

IKE automatically negotiates IPSec security associations (SAs) and enables IPSec secure communications without costly manual preconfiguration. Specifically, IKE provides these benefits:

•Eliminates the need to manually specify all the IPSec security parameters in the crypto maps at both peers.
•Allows you to specify a lifetime for the IPSec security association.
•Allows encryption keys to change during IPSec sessions.
•Allows IPSec to provide anti-replay services.
•Permits certification authority (CA) support for a manageable, scalable IPSec implementation.
•Allows dynamic authentication of peers.

About ISAKMP
The Internet Security Association and Key Management Protocol (ISAKMP) is a framework that defines the phases for establishing a secure relationship and support for negotiation of security attributes, it does not establish sessions keys by itself, it is used along with the Oakley session key establishment protocol. The Secure Key Exchange Mechanism (SKEME) describes a secure exchange mechanism and Oakley defines the modes of operation needed to establish a secure connection.

ISAKMP provides a framework for Internet key management and provides the specific protocol support for negotiation of security attributes. Alone, it does not establish session keys. However it can be used with various session key establishment protocols, such as Oakley, to provide a complete solution to Internet key management.
About Oakley
The Oakley protocol uses a hybrid Diffie-Hellman technique to establish session keys on Internet hosts and routers. Oakley provides the important security property of Perfect Forward Secrecy (PFS) and is based on cryptographic techniques that have survived substantial public scrutiny. Oakley can be used by itself, if no attribute negotiation is needed, or Oakley can be used in conjunction with ISAKMP. When ISAKMP is used with Oakley, key escrow is not feasible.

The ISAKMP and Oakley protocols have been combined into a hybrid protocol. The resolution of ISAKMP with Oakley uses the framework of ISAKMP to support a subset of Oakley key exchange modes. This new key exchange protocol provides optional PFS, full security association attribute negotiation, and authentication methods that provide both repudiation and non-repudiation. Implementations of this protocol can be used to establish VPNs and also allow for users from remote sites (who may have a dynamically allocated IP address) access to a secure network.

About IPSec
The IETF's IPSec Working Group develops standards for IP-layer security mechanisms for both IPv4 and IPv6. The group also is developing generic key management protocols for use on the Internet. For more information, refer to the IP Security and Encryption Overview.

IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF) that provides security for transmission of sensitive information over unprotected networks such as the Internet. It acts at the network level and implements the following standards:

IPSec
Internet Key Exchange (IKE)
Data Encryption Standard (DES)
MD5 (HMAC variant)
SHA (HMAC variant)
Authentication Header (AH)
Encapsulating Security Payload (ESP)

IPSec services provide a robust security solution that is standards-based. IPSec also provides data authentication and anti-replay services in addition to data confidentiality services.

For more information regarding IPSec, refer to the chapter "Configuring IPSec Network Security."

About SKEME
SKEME constitutes a compact protocol that supports a variety of realistic scenarios and security models over Internet. It provides clear tradeoffs between security and performance as required by the different scenarios without incurring in unnecessary system complexity. The protocol supports key exchange based on public key, key distribution centers, or manual installation, and provides for fast and secure key refreshment. In addition, SKEME selectively provides perfect forward secrecy, allows for replaceability and negotiation of the underlying cryptographic primitives, and addresses privacy issues as anonymity and repudiatability

SKEME's basic mode is based on the use of public keys and a Diffie-Hellman shared secret generation.

However, SKEME is not restricted to the use of public keys, but also allows the use of a pre-shared key. This key can be obtained by manual distribution or by the intermediary of a key distribution center (KDC) such as Kerberos.

In short, SKEME contains four distinct modes:

Basic mode, which provides a key exchange based on public keys and ensures PFS thanks to Diffie-Hellman.
A key exchange based on the use of public keys, but without Diffie-Hellman.
A key exchange based on the use of a pre-shared key and on Diffie-Hellman.
A mechanism of fast rekeying based only on symmetrical algorithms.

In addition, SKEME is composed of three phases: SHARE, EXCH and AUTH.

During the SHARE phase, the peers exchange half-keys, encrypted with their respective public keys. These two half-keys are used to compute a secret key K. If anonymity is wanted, the identities of the two peers are also encrypted. If a shared secret already exists, this phase is skipped.
The exchange phase (EXCH) is used, depending on the selected mode, to exchange either Diffie-Hellman public values or nonces. The Diffie-Hellman shared secret will only be computed after the end of the exchanges.
The public values or nonces are authenticated during the authentication phase (AUTH), using the secret key established during the SHARE phase.

The messages from these three phases do not necessarily follow the order described above; in actual practice they are combined to minimize the number of exchanged messages.
References used for this question:

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 172).

http://tools.ietf.org/html/rfc4306
http://tools.ietf.org/html/rfc4301
http://en.wikipedia.org/wiki/Internet_Key_Exchange

CISCO ISAKMP and OAKLEY information
CISCO Configuring Internet Key Exchange Protocol http://www.hsc.fr/ressources/articles/ipsec-tech/index.html.en

QUESTION 389
Which of the following binds a subject name to a public key value?

A. A public-key certificate
B. A public key infrastructure
C. A secret key infrastructure
D. A private key certificate

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Remember the term Public-Key Certificate is synonymous with Digital Certificate or Identity certificate.

The certificate itself provides the binding but it is the certificate authority who will go through the Certificate Practice Statements (CPS) actually validating the bindings and vouch for the identity of the owner of the key within the certificate.

As explained in Wikipedia:
In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document which uses a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme such as PGP or GPG, the signature is of either the user (a self-signed certificate) or other users ("endorsements") by getting people to sign each other keys. In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together. RFC 2828 defines the certification authority (CA) as:

An entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

An authority trusted by one or more users to create and assign certificates. Optionally, the certification authority may create the user's keys.

X509 Certificate users depend on the validity of information provided by a certificate. Thus, a CA should be someone that certificate users trust, and usually holds an official position created and granted power by a government, a corporation, or some other organization. A CA is responsible for managing the life cycle of certificates and, depending on the type of certificate and the CPS that applies, may be responsible for the life cycle of key pairs associated with the certificates

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Public_key_certificate

QUESTION 390
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?

A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate

Correct Answer: B

Section: Cryptography
Explanation

Explanation/Reference:
The Internet Security Glossary (RFC2828) defines an attribute certificate as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its publickey certificates.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 391
What can be defined as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire?

A. Certificate revocation list
B. Certificate revocation tree
C. Authority revocation list
D. Untrusted certificate list

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The Internet Security Glossary (RFC2828) defines the Authority Revocation List (ARL) as a data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire.

Do not to confuse with an ARL with a Certificate Revocation List (CRL). A certificate revocation list is a mechanism for distributing notices of certificate revocations. The question specifically mentions "issued to CAs" which makes ARL a better answer than CRL.
http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-29.asp
$ certificate revocation list (CRL)
(I) A data structure that enumerates digital certificates that have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 certificate revocation list.) http://rfclibrary.hosting.com/rfc/rfc2828/rfc2828-17.asp
$ authority revocation list (ARL)
(I) A data structure that enumerates digital certificates that were issued to CAs but have been invalidated by their issuer prior to when they were scheduled to expire. (See: certificate expiration, X.509 authority revocation list.)

In a few words: We use CRL's for end-user cert revocation and ARL's for CA cert revocation - both can be placed in distribution points.

QUESTION 392
What is the name of the third party authority that vouches for the binding between the data items in a digital certificate?

A. Registration authority
B. Certification authority
C. Issuing authority
D. Vouching authority

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
A certification authority (CA) is a third party entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate. An issuing authority could be considered a correct answer, but not the best answer, since it is too generic. Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 393
What enables users to validate each other's certificate when they are certified under different certification hierarchies?

A. Cross-certification
B. Multiple certificates
C. Redundant certification authorities
D. Root certification authorities

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Cross-certification is the act or process by which two CAs each certifiy a public key of the other, issuing a public-key certificate to that other CA, enabling users that are certified under different certification hierarchies to validate each other's certificate.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 394

Which of the following would best define a digital envelope?

A. A message that is encrypted and signed with a digital certificate.
B. A message that is signed with a secret key and encrypted with the sender's private key.
C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.
D. A message that is encrypted with the recipient's public key and signed with the sender's private key.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
A digital envelope for a recipient is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.

It consists of a hybrid encryption scheme in sealing a message, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that one else can open the message.

In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm and the public key of the intended recipient.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 395
What can be defined as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity?

A. A digital envelope
B. A cryptographic hash
C. A Message Authentication Code
D. A digital signature

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines a digital signature as a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity.

The steps to create a Digital Signature are very simple:
1. You create a Message Digest of the message you wish to send
2. You encrypt the message digest using your Private Key which is the action of Signing
3. You send the Message along with the Digital Signature to the recipient

To validate the Digital Signature the recipient will make use of the sender Public Key. Here are the steps:
1. The receiver will decrypt the Digital Signature using the sender Publick Key producing a clear text message digest.
2. The receiver will produce his own message digest of the message received.
3. At this point the receiver will compare the two message digest (the one sent and the one produce by the receiver), if the two matches, it proves the authenticity of the message and it confirms that the message was not modified in transit validating the integrity as well. Digital Signatures provides for Authenticity and Integrity only. There is no confidentiality in place, if you wish to get confidentiality it would be needed for the sender to encrypt everything with the receiver public key as a last step before sending the message.

A Digital Envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient. In simple term it is a type of security that uses two layers of encryption to protect a message. First, the message itself is encoded using symmetric encryption, and then the key to decode the message is encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead.
A cryptographic hash is the result of a cryptographic hash function such as MD5, SHA-1, or SHA-2. A hash value also called a Message Digest is like a fingerprint of a message. It is used to proves integrity and ensure the message was not changed either in transit or in storage.

A Message Authentication Code (MAC) refers to an ANSI standard for a checksum that is computed with a keyed hash that is based on DES or it can also be produced without using DES by concataning the Secret Key at the end of the message (simply adding it at the end of the message) being sent and then producing a Message digest of the Message+Secret Key together. The MAC is then attached and sent along with the message but the Secret Key is NEVER sent in clear text over the network.

In cryptography, HMAC (Hash-based Message Authentication Code), is a specific construction for calculating a message authentication code (MAC) involving a cryptographic hash function in combination with a secret key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-1, may be used in the calculation of an HMAC; the resulting MAC algorithm is termed HMACMD5 or HMAC-SHA1 accordingly. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, the size of its hash output length in bits and on the size and quality of the cryptographic key.

There is more than one type of MAC: Meet CBC-MAC
In cryptography, a Cipher Block Chaining Message Authentication Code, abbreviated CBC-MAC, is a technique for constructing a message authentication code from a block cipher. The message is encrypted with some block cipher algorithm in CBC mode to create a chain of blocks such that each block depends on the proper encryption of the previous block. This interdependence ensures that a change to any of the plaintext bits will cause the final encrypted block to change in a way that cannot be predicted or counteracted without knowing the key to the block cipher.

References:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

and

http://www.webopedia.com/TERM/D/digital_envelope.htm
l and http://en.wikipedia.org/wiki/CBC-MAC

QUESTION 396
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 397
Which of the following is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism?

A. OAKLEY
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. IPsec Key exchange (IKE)

Correct Answer: B

Section: Cryptography
Explanation
Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines the Internet Security Association and Key Management Protocol (ISAKMP) as an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Let's clear up some confusion here first. Internet Key Exchange (IKE) is a hybrid protocol, it consists of 3 "protocols"

ISAKMP: It's not a key exchange protocol per se, it's a framework on which key exchange protocols operate. ISAKMP is part of IKE. IKE establishs the shared security policy and authenticated keys. ISAKMP is the protocol that specifies the mechanics of the key exchange.

Oakley: Describes the "modes" of key exchange (e.g. perfect forward secrecy for keys, identity protection, and authentication). Oakley describes a series of key exchanges and services.

SKEME: Provides support for public-key-based key exchange, key distribution centres, and manual installation, it also outlines methods of secure and fast key refreshment.

So yes, IPSec does use IKE, but ISAKMP is part of IKE.
The questions did not ask for the actual key negotiation being done but only for the "exchange of key generation and authentication data" being done. Under Oakly it would be Diffie Hellman (DH) that would be used for the actual key nogotiation.

The following are incorrect answers:

Simple Key-management for Internet Protocols (SKIP) is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

OAKLEY is a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.

IPsec Key Exchange (IKE) is an Internet, IPsec, key-establishment protocol [R2409] (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.
Reference used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 398
Which of the following is defined as a key establishment protocol based on the Diffie-Hellman algorithm proposed for IPsec but superseded by IKE?

A. Diffie-Hellman Key Exchange Protocol

B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Simple Key-management for Internet Protocols (SKIP)
D. OAKLEY

Correct Answer: D
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines OAKLEY as a key establishment protocol (proposed for IPsec but superseded by IKE) based on the Diffie-Hellman algorithm and designed to be a compatible component of ISAKMP.

ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

ISAKMP provides a framework for authentication and key exchange but does not define them. ISAKMP is designed to be key exchange independant; that is, it is designed to support many different key exchanges.
Oakley and SKEME each define a method to establish an authenticated key exchange. This includes payloads construction, the information payloads carry, the order in which they are processed and how they are used.

Oakley describes a series of key exchanges-- called modes and details the services provided by each (e.g. perfect forward secrecy for keys, identity protection, and authentication).

SKEME describes a versatile key exchange technique which provides anonymity, repudiability, and quick key refreshment.

RFC 2049 describes the IKE protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material for use with ISAKMP, and for other security associations such as AH and ESP for the IETF IPsec DOI.
While Oakley defines "modes", ISAKMP defines "phases". The relationship between the two is very straightforward and IKE presents different exchanges as modes which operate in one of two phases.

Phase 1 is where the two ISAKMP peers establish a secure, authenticated channel with which to communicate. This is called the ISAKMP Security Association (SA). "Main Mode" and "Aggressive Mode" each accomplish a phase 1 exchange. "Main Mode" and "Aggressive Mode" MUST ONLY be used in phase 1.

Phase 2 is where Security Associations are negotiated on behalf of services such as IPsec or any other service which needs key material and/or parameter negotiation. "Quick Mode" accomplishes a phase 2 exchange. "Quick Mode" MUST ONLY be used in phase 2.

References:

CISSP: Certified Information Systems Security Professional Study Guide By James Michael Stewart, Ed Tittel, Mike Chappl, page 397

RFC 2049 at: http://www.ietf.org/rfc/rfc2409
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
The All-in-one CISSP Exam Guide, 3rd Edition, by Shon Harris, page 674
The CISSP and CAP Prep Guide, Platinum Edition, by Krutz and Vines

QUESTION 399
Which of the following is defined as an Internet, IPsec, key-establishment protocol, partly based on OAKLEY, that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations?

A. Internet Key exchange (IKE)
B. Security Association Authentication Protocol (SAAP)
C. Simple Key-management for Internet Protocols (SKIP)
D. Key Exchange Algorithm (KEA)

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines IKE as an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

The following are incorrect answers:

SKIP is a key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

The Key Exchange Algorithm (KEA) is defined as a key agreement algorithm that is similar to the Diffie-Hellman algorithm, uses 1024-bit asymmetric keys, and was developed and formerly classified at the secret level by the NSA.

Security Association Authentication Protocol (SAAP) is a distracter.

Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 400
Which of the following can best be defined as a key distribution protocol that uses hybrid encryption to convey session keys. This protocol establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis?

A. Internet Security Association and Key Management Protocol (ISAKMP)
B. Simple Key-management for Internet Protocols (SKIP)
C. Diffie-Hellman Key Distribution Protocol
D. IPsec Key exchange (IKE)

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
RFC 2828 (Internet Security Glossary) defines Simple Key Management for Internet Protocols (SKIP) as:

A key distribution protocol that uses hybrid encryption to convey session keys that are used to encrypt data in IP packets.

SKIP is an hybrid Key distribution protocol similar to SSL, except that it establishes a long-term key once, and then requires no prior communication in order to establish or exchange keys on a session-by-session basis. Therefore, no connection setup overhead exists and new keys values are not continually generated. SKIP uses the knowledge of its own secret key or private component and the destination's public component to calculate a unique key that can only be used between them.

IKE stand for Internet Key Exchange, it makes use of ISAKMP and OAKLEY internally.
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

The following are incorrect answers:

ISAKMP is an Internet IPsec protocol to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

IKE is an Internet, IPsec, key-establishment protocol (partly based on OAKLEY) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP.

IPsec Key exchange (IKE) is only a detracto.

Reference(s) used for this question:
SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol
and http://en.wikipedia.org/wiki/Simple_Key-Management_for_Internet_Protocol

QUESTION 401
Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?

A. A known-plaintext attack
B. A known-algorithm attack
C. A chosen-ciphertext attack
D. A chosen-plaintext attack

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
RFC2828 (Internet Security Glossary) defines a known-plaintext attack as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as the knowing the cryptographic algorithm). A chosen-ciphertext attack is defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst. A chosen-plaintext attack is a cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst. The other choice is a distracter.

The following are incorrect answers:

A chosen-plaintext attacks
The attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext. This gives her more power and possibly a deeper understanding of the way the encryption process works so she can gather more information about the key being used. Once the key is discovered, other messages encrypted with that key can be decrypted.

A chosen-ciphertext attack
In chosen-ciphertext attacks, the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext. Again, the goal is to figure out the key. This is a harder attack to carry out compared to the previously mentioned attacks, and the attacker may need to have control of the system that contains the cryptosystem.

A known-algorithm attack
Knowing the algorithm does not give you much advantage without knowing the key. This is a bogus detractor. The algorithm should be public, which is the Kerckhoffs's Principle . The only secret should be the key.

Reference(s) used for this question:

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
and
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 866). McGraw-Hill. Kindle Edition.
and

Kerckhoffs's Principle

QUESTION 402
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.

A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main or significant properties:

it is easy (but not necessarily quick) to compute the hash value for any given message it is infeasible to generate a message that has a given hash it is infeasible to modify a message without changing the hash it is infeasible to find two different messages with the same hash

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

Source:

TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
and
http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 403
The Data Encryption Algorithm performs how many rounds of substitution and permutation?

A. 4
B. 16C. 54
D. 64

Correct Answer: B
Section: Cryptography
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 404
Which of the following statements is most accurate regarding a digital signature?

A. It is a method used to encrypt confidential data.
B. It is the art of transferring handwritten signature to electronic media.
C. It allows the recipient of data to prove the source and integrity of data.

D. It can be used as a signature system and a cryptosystem.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 405
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as "_____," RSA is quite feasible for computer use.

A. computing in Galois fields
B. computing in Gladden fields
C. computing in Gallipoli fields
D. computing in Galbraith fields

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as computing in Galois fields, RSA is quite feasible for computer use.
Source: FITES, Philip E., KRATZ, Martin P., Information Systems Security: A Practitioner's Reference, 1993, Van Nostrand Reinhold, page 44.

QUESTION 406
Which of the following concerning the Rijndael block cipher algorithm is false?

A. The design of Rijndael was strongly influenced by the design of the block cipher Square.
B. A total of 25 combinations of key length and block length are possible C. Both block size and key length can be extended to multiples of 64 bits.
D. The cipher has a variable block length and key length.

Correct Answer: C
Section: Cryptography
Explanation

Explanation/Reference:
The answer above is the correct answer because it is FALSE. Rijndael does not support multiples of 64 bits but multiples of 32 bits in the range of 128 bits to 256 bits. Key length could be 128, 160, 192, 224, and 256.

Both block length and key length can be extended very easily to multiples of 32 bits. For a total combination of 25 different block and key size that are possible.

The Rijndael Cipher
Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen as a candidate algorithm for the Advanced Encryption Standard (AES) in the United States of America. The cipher has a variable block length and key length.

Rijndael can be implemented very efficiently on a wide range of processors and in hardware.

The design of Rijndael was strongly influenced by the design of the block cipher Square.

The Advanced Encryption Standard (AES)
The Advanced Encryption Standard (AES) keys are defined to be either 128, 192, or 256 bits in accordance with the requirements of the AES.

The number of rounds, or iterations of the main algorithm, can vary from 10 to 14 within the Advanced Encryption Standard (AES) and is dependent on the block size and key length. 128 bits keys uses 10 rounds or encryptions, 192 bits keys uses 12 rounds of encryption, and 256 bits keys uses 14 rounds of encryption.

The low number of rounds has been one of the main criticisms of Rijndael, but if this ever becomes a problem the number of rounds can easily be increased at little extra cost performance wise by increasing the block size and key length.

Range of key and block lengths in Rijndael and AES
Rijndael and AES differ only in the range of supported values for the block length and cipher key length.

For Rijndael, the block length and the key length can be independently specified to any multiple of 32 bits, with a minimum of 128 bits, and a maximum of 256 bits. The support for block and key lengths 160 and 224 bits was introduced in Joan Daemen and Vincent Rijmen, AES submission document on Rijndael, Version 2, September 1999 available at http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf

AES fixes the block length to 128 bits, and supports key lengths of 128, 192 or 256 bits only.

Reference used for this question:
The Rijndael Page
and
http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf
and
FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

QUESTION 407
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I ?

A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well. Designers of tamper-resistant cryptographic smart cards must be particularly cognizant of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.

According to RSA:
Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key.

A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.

A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books.

A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext and then obtain the corresponding encrypted ciphertext. A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished:

Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".

Adaptive chosen-plaintext attack, is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions. The cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

Non-randomized (deterministic) public key encryption algorithms are vulnerable to simple "dictionary"-type attacks, where the attacker builds a table of likely messages and their corresponding ciphertexts. To find the decryption of some observed ciphertext, the attacker simply looks the ciphertext up in the table. As a result, public-key definitions of security under chosen-plaintext attack require probabilistic encryption (i.e., randomized encryption). Conventional symmetric ciphers, in which the same key is used to encrypt and decrypt a text, may also be vulnerable to other forms of chosen-plaintext attack, for example, differential cryptanalysis of block ciphers.

An adaptive-chosen-ciphertext is the adaptive version of the above attack. A cryptanalyst can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).

The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosenciphertexts are generally applicable only when they have the property of ciphertext malleability — that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.

A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.

References:
RSA Laboratories FAQs about today's cryptography: What are some of the basic types of cryptanalytic attack?

also see:
http://www.giac.org/resources/whitepaper/cryptography/57.php
and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

QUESTION 408
What is NOT true about a one-way hashing function?

A. It provides authentication of the message
B. A hash cannot be reverse to get the message used to create the hash
C. The results of a one-way hash is a message digest
D. It provides integrity of the message

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
A one way hashing function can only be use for the integrity of a message and not for authentication or confidentiality. Because the hash creates just a fingerprint of the message which cannot be reversed and it is also very difficult to create a second message with the same hash.

A hash by itself does not provide Authentication. It only provides a weak form or integrity. It would be possible for an attacker to perform a Man-In-The-Middle attack where both the hash and the digest could be changed without the receiver knowing it.

A hash combined with your session key will produce a Message Authentication Code (MAC) which will provide you with both authentication of the source and integrity. It is sometimes referred to as a Keyed Hash.
A hash encrypted with the sender private key produce a Digital Signature which provide authentication, but not the hash by itself.
Hashing functions by themselves such as MD5, SHA1, SHA2, SHA-3 does not provide authentication.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 548

QUESTION 409
You work in a police department forensics lab where you examine computers for evidence of crimes. Your work is vital to the success of the prosecution of criminals.

One day you receive a laptop and are part of a two man team responsible for examining it together. However, it is lunch time and after receiving the laptop you leave it on your desk and you both head out to lunch.

What critical step in forensic evidence have you forgotten?

A. Chain of custody
B. Locking the laptop in your desk
C. Making a disk image for examination
D. Cracking the admin password with chntpw

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
When evidence from a crime is to be used in the prosecution of a criminal it is critical that you follow the law when handling that evidence. Part of that process is called chain of custody and is when you maintain proactive and documented control over ALL evidence involved in a crime.

Failure to do this can lead to the dismissal of charges against a criminal because if the evidence is compromised because you failed to maintain of chain of custody.

A chain of custody is chronological documentation for evidence in a particular case, and is especially important with electronic evidence due to the possibility of fraudulent data alteration, deletion, or creation. A fully detailed chain of custody report is necessary to prove the physical custody of a piece of evidence and show all parties that had access to said evidence at any given time.

Evidence must be protected from the time it is collected until the time it is presented in court.

The following answers are incorrect:

- Locking the laptop in your desk: Even this wouldn't assure that the defense team would try to challenge chain of custody handling. It's usually easy to break into a desk drawer and evidence should be stored in approved safes or other storage facility.

- Making a disk image for examination: This is a key part of system forensics where we make a disk image of the evidence system and study that as opposed to studying the real disk drive. That could lead to loss of evidence. However if the original evidence is not secured than the chain of custoday has not been maintained properly.

- Cracking the admin password with chntpw: This isn't correct. Your first mistake was to compromise the chain of custody of the laptop. The chntpw program is a Linux utility to (re)set the password of any user that has a valid (local) account on a Windows system, by modifying the crypted password in the registry's SAM file. You do not need to know the old password to set a new one. It works offline which means you must have physical access (i.e., you have to shutdown your computer and boot off a linux floppy disk). The bootdisk includes stuff to access NTFS partitions and scripts to glue the whole thing together. This utility works with SYSKEY and includes the option to turn it off. A bootdisk image is provided on their website at http://freecode.com/projects/chntpw .

The following reference(s) was used to create this question:

For more details and to cover 100% of the exam Qs, subscribe to our holistic Security+ 2014 CBT Tutorial at: http://www.cccure.tv/
and
http://en.wikipedia.org/wiki/Chain_of_custody and
http://www.datarecovery.com/forensic_chain_of_custody.as
p

QUESTION 410
When we encrypt or decrypt data there is a basic operation involving ones and zeros where they are compared in a process that looks something like this:

0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output

What is this cryptographic operation called?

A. Exclusive-OR
B. Bit Swapping
C. Logical-NOR
D. Decryption

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:

When we encrypt data we are basically taking the plaintext information and applying some key material or keystream and conducting something called an XOR or Exclusive-OR operation.

The symbol used for XOR is the following: This is a type of cipher known as a stream cipher.

The operation looks like this:
0101 0001 Plain text
0111 0011 Key stream
0010 0010 Output (ciphertext)

As you can see, it's not simple addition and the XOR Operation uses something called a truth table that explains why 0+1=1 and 1+1=0.

The rules are simples, if both bits are the same the result is zero, if both bits are not the same the result is one.

The following answers are incorrect:

- Bit Swapping: Incorrect. This isn't a known cryptographic operations.

- Logical NOR: Sorry, this isn't correct but is where only 0+0=1. All other combinations of 1+1, 1+0 equals 0. More on NOR here.

- Decryption: Sorry, this is the opposite of the process of encryption or, the process of applying the keystream to the plaintext to get the resulting encrypted text.

The following reference(s) was used to create this question:

For more details on XOR and all other Qs of cryptography. Subscribe to our holistic Security+ CBT tutorial at http://www.cccure.tv
and
http://en.wikipedia.org/wiki/Exclusive-or
and
http://en.wikipedia.org/wiki/Stream_cipher

QUESTION 411
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?

A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)

Correct Answer: A

Section: Cryptography
Explanation

Explanation/Reference:
OTP or One Time Pad is considered unbreakable if the key is truly random and is as large as the plaintext and never reused in whole or part AND kept secret.

In cryptography, a one-time pad is a system in which a key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using the matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected.

With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one-time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.

One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.

The biggest challenge with OTP was to get the pad security to the person or entity you wanted to communicate with. It had to be done in person or using a trusted courrier or custodian. It certainly did not scale up very well and it would not be usable for large quantity of data that needs to be encrypted as we often time have today.

The following answers are incorrect:

- One time Cryptopad: Almost but this isn't correct. Cryptopad isn't a valid term in cryptography.

- Cryptanalysis: Sorry, incorrect. Cryptanalysis is the process of analyzing information in an effort to breach the cryptographic security systems.

- PGP - Pretty Good Privacy: PGP, written by Phil Zimmermann is a data encryption and decryption program that provides cryptographic privacy and authentication for data. Still isn't the right answer though. Read more here about PGP.

The following reference(s) was used to create this question:

To get more info on this Qs or any Qs of Security+, subscribe to the CCCure Holistic Security+ CBT available at: http://www.cccure.tv
and
http://users.telenet.be/d.rijmenants/en/otp.htm
and
http://en.wikipedia.org/wiki/One-time_pad
and

http://searchsecurity.techtarget.com/definition/one-time-pad

QUESTION 412
Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?

A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.

Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.

In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session.

The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.

The following answers are incorrect:

- Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.

- OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.

- Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)

The following reference(s) was used to create this question:

For more details on this TOPIC and other Qs of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at http://www.cccure.tv
and
whatis.techtarget.com/definition/initialization-vector-IV
and
en.wikipedia.org/wiki/Initialization_vector

QUESTION 413
Which of the following terms can be described as the process to conceal data into another file or media in a practice known as security through obscurity?

A. Steganography
B. ADS - Alternate Data Streams
C. Encryption
D. NTFS ADS

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message or could claim there is a message.

It is a form of security through obscurity.

The word steganography is of Greek origin and means "concealed writing." It combines the Greek words steganos (στεγανός), meaning "covered or protected," and graphei (γραφή) meaning "writing."

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable, will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

It is sometimes referred to as Hiding in Plain Sight. This image of trees blow contains in it another image of a cat using Steganography.
ADS Tree with Cat inside

This image below is hidden in the picture of the trees above:

Hidden Kitty
As explained here the image is hidden by removing all but the two least significant bits of each color component and subsequent normalization.

ABOUT MSF and LSF

One of the common method to perform steganography is by hiding bits within the Least Significant Bits of a media (LSB) or what is sometimes referred to as Slack Space. By modifying only the least significant bit, it is not possible to tell if there is an hidden message or not looking at the picture or the media. If you would change the Most Significant Bits (MSB) then it would be possible to view or detect the changes just by looking at the picture. A person can perceive only up to 6 bits of depth, bit that are changed past the first sixth bit of the color code would be undetectable to a human eye.

If we make use of a high quality digital picture, we could hide six bits of data within each of the pixel of the image. You have a color code for each pixel composed of a Red, Green, and Blue value. The color code is 3 sets of 8 bits each for each of the color. You could change the last two bit to hide your data. See below a color code for one pixel in binary format. The bits below are not real they are just example for illustration purpose:

RED	GREEN	BLUE
0101 0101	1100 1011	1110 0011
MSB LSB	MSB LSB	MSB LSB

Let's say that I would like to hide the letter A uppercase within the pixels of the picture. If we convert the letter "A" uppercase to a decimal value it would be number 65 within the ASCII table , in binary format the value 65 would translet to 01000001

You can break the 8 bits of character A uppercase in group of two bits as follow: 01 00 00 01

Using the pixel above we will hide those bits within the last two bits of each of the color as follow:

RED	GREEN	BLUE
0101 0101	1100 1000	1110 0000
MSB LSB	MSB LSB	MSB LSB

As you can see above, the last two bits of RED was already set to the proper value of 01, then we move to the GREEN value and we changed the last two bit from
11 to 00, and finally we changed the last two bits of blue to 00. One pixel allowed us to hide 6 bits of data. We would have to use another pixel to hide the remaining two bits.

The following answers are incorrect:

- ADS - Alternate Data Streams: This is almost correct but ADS is different from steganography in that ADS hides data in streams of communications or files while Steganography hides data in a single file.

- Encryption: This is almost correct but Steganography isn't exactly encryption as much as using space in a file to store another file.

- NTFS ADS: This is also almost correct in that you're hiding data where you have space to do so. NTFS, or New Technology File System common on Windows computers has a feature where you can hide files where they're not viewable under normal conditions. Tools are required to uncover the ADS-hidden files.

The following reference(s) was used to create this question:
The CCCure Security+ Holistic Tutorial at http://www.cccure.tv
and
Steganography tool
and
http://en.wikipedia.org/wiki/Steganography

QUESTION 414
Which of the following type of cryptography is used when both parties use the same key to communicate securely with each other?

A. Symmetric Key Cryptography
B. PKI - Public Key Infrastructure
C. Diffie-Hellman
D. DSS - Digital Signature Standard

Correct Answer: A
Section: Cryptography
Explanation

Explanation/Reference:
Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext (sender) and decryption of ciphertext (receiver). The keys may be identical, in practice, they represent a shared secret between two or more parties that can be used to maintain a private information link.

This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. This is also known as secret key encryption. In symmetric key cryptography, each end of the conversation must have the same key or they cannot decrypt the message sent to them by the other party.

Symmetric key crypto is very fast but more difficult to manage due to the need to distribute the key in a secure means to all parts needing to decrypt the data. There is no key management built within Symmetric crypto.

PKI provides CIA - Confidentiality (Through encryption) Integrity (By guaranteeing that the message hasn't change in transit) and Authentication (Non-repudiation). Symmetric key crypto provides mostly Confidentiality.

The following answers are incorrect:

- PKI - Public Key Infrastructure: This is the opposite of symmetric key crypto. Each side in PKI has their own private key and public key. What one key encrypt the other one can decrypt. You make use of the receiver public key to communicate securely with a remote user. The receiver will use their matching private key to decrypt the data.

- Diffie-Hellman: Sorry, this is an asymmetric key technique. It is used for key agreement over an insecure network such as the Internet. It allows two parties who has never met to negotiate a secret key over an insecure network while preventing Man-In-The-Middle (MITM) attacks.

- DSS - Digital Signature Standard: Sorry, this is an asymmetric key technique.

The following reference(s) was used to create this question:
To learn more about this Qs and 100% of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) on our Learning Management System at:
http://www.cccure.tv
and
http://en.wikipedia.org/wiki/Symmetric-key_algorithm

QUESTION 415
Which of the following is true of network security?

A. A firewall is a not a necessity in today's connected world.
B. A firewall is a necessity in today's connected world.
C. A whitewall is a necessity in today's connected world.
D. A black firewall is a necessity in today's connected world.

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Commercial firewalls are a dime-a-dozen in todays world. Black firewall and whitewall are just distracters.

QUESTION 416
What is called the access protection system that limits connections by calling back the number of a previously authorized location?

A. Sendback systems

B. Callback forward systems
C. Callback systems
D. Sendback forward systems

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The Answer: Call back Systems; Callback systems provide access protection by calling back the number of a previously authorized location, but this control can be compromised by call forwarding.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 35.

QUESTION 417
What is a decrease in amplitude as a signal propagates along a transmission medium best known as?

A. Crosstalk
B. Noise
C. Delay distortion
D. Attenuation

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Attenuation is the loss of signal strength as it travels. The longer a cable, the more at tenuation occurs, which causes the signal carrying the data to deteriorate. This is why standards include suggested cable-run lengths. If a networking cable is too long, attenuation may occur. Basically, the data are in the form of electrons, and these electrons have to “swim” through a copper wire. However, this is more like swimming upstream, because there is a lot of resistance on the electrons working in this media. After a certain distance, the electrons start to slow down and their encoding format loses form. If the form gets too degraded, the receiving system cannot interpret them any longer. If a network administrator needs to run a cable longer than its recommended segment length, she needs to insert a repeater or some type of device that will amplify the signal and ensure it gets to its destination in the right encoding format.
Attenuation can also be caused by cable breaks and malfunctions. This is why cables should be tested. If a cable is suspected of attenuation problems, cable testers can inject signals into the cable and read the results at the end of the cable.

The following answers are incorrect:

Crosstalk - Crosstalk is one example of noise where unwanted electrical coupling between adjacent lines causes the signal in one wire to be picked up by the signal in an adjacent wire.

Noise - Noise is also a signal degradation but it refers to a large amount of electrical fluctuation that can interfere with the interpretation of the signal by the receiver.

Delay distortion - Delay distortion can result in a misinterpretation of a signal that results from transmitting a digital signal with varying frequency components. The various components arrive at the receiver with varying delays.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 265
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 &
CISSP All-In-One Exam guide 6th Edition Page Number 561

QUESTION 418
Which device acting as a translator is used to connect two networks or applications from layer 4 up to layer 7 of the ISO/OSI Model?

A. Bridge
B. Repeater
C. Router
D. Gateway

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A gateway is used to connect two networks using dissimilar protocols at the lower layers or it could also be at the highest level of the protocol stack.

Important Note:
For the purpose of the exam, you have to remember that a gateway is not synonymous to the term firewall.

The second thing you must remembers is the fact that a gateway act as a translation device.

It could be used to translate from IPX to TCP/IP for example. It could be used to convert different types of applications protocols and allow them to communicate together. A gateway could be at any of the OSI layers but usually tend to be higher up in the stack.

For your exam you should know the information below:

Repeaters
A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.
Repeaters can also work as line conditioners by actually cleaning up the signals. This works much better when amplifying digital signals than when amplifying analog signals, because digital signals are discrete units, which makes extraction of background noise from them much easier for the amplifier. If the device is amplifying analog signals, any accompanying noise often is amplified as well, which may further distort the signal.
A hub is a multi-port repeater. A hub is often referred to as a concentrator because it is the physical communication device that allows several computers and devices to communicate with each other. A hub does not understand or work with IP or MAC addresses. When one system sends a signal to go to another system connected to it, the signal is broadcast to all the ports, and thus to all the systems connected to the concentrator.

Repeater

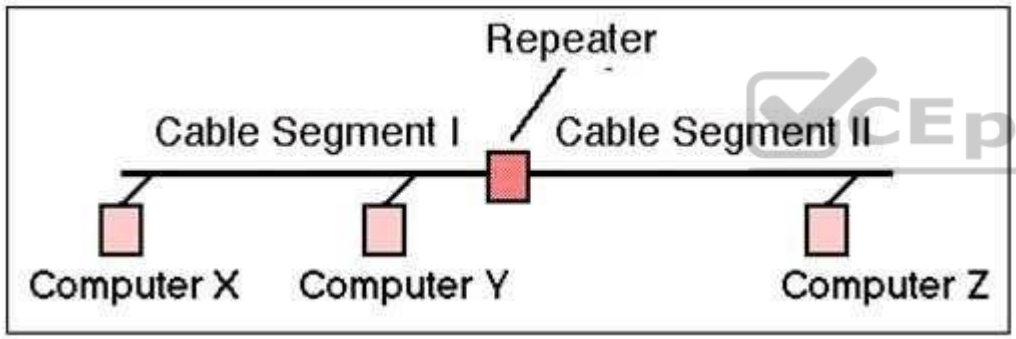


Image Reference- http://www.erg.abdn.ac.uk/~gorry/course/images/repeater.gif

Bridges
A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Bridge

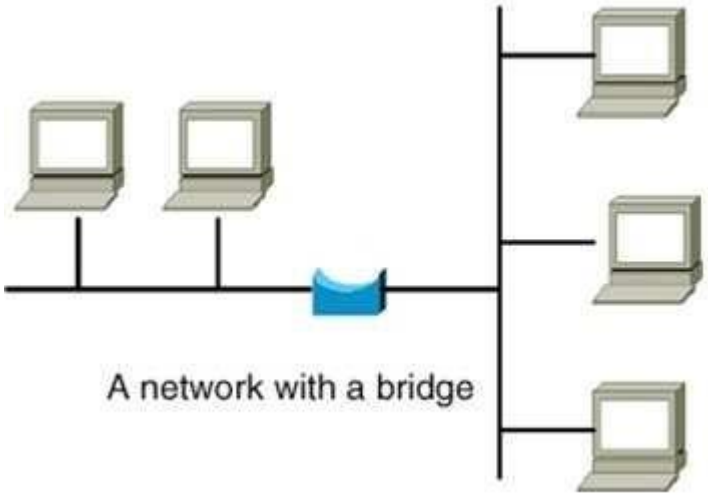


Image Reference- http://www.oreillynet.com/network/2001/01/30/graphics/bridge.jpg

Routers

Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary. Because routers have more network-level knowledge, they can perform higher-level functions, such as calculating the shortest and most economical path between the sending and receiving hosts.

Router and Switch

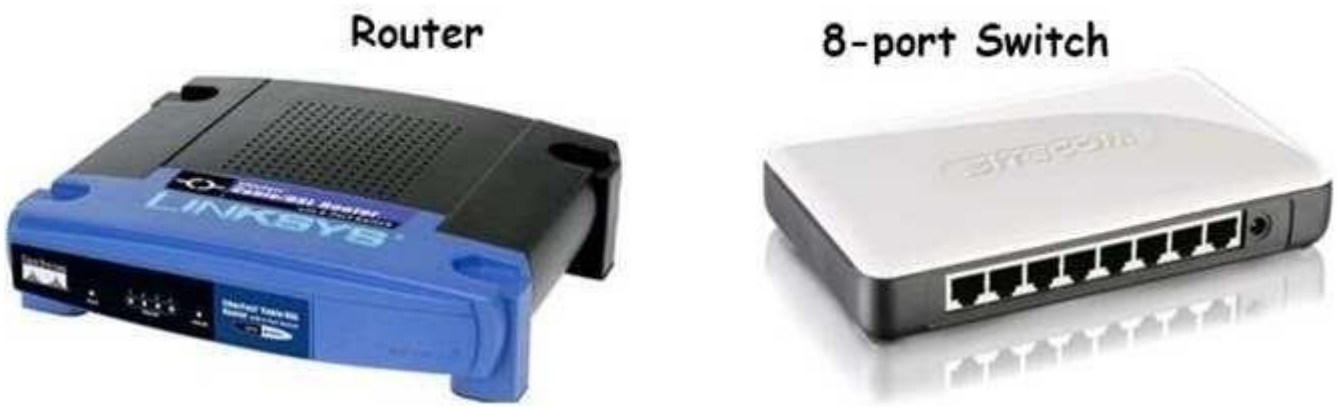


Image Reference- http://www.computer-networking-success.com/images/router-switch.jpg

Switches

Switches combine the functionality of a repeater and the functionality of a bridge. A switch amplifies the electrical signal, like a repeater, and has the built-in circuitry and intelligence of a bridge. It is a multi-port connection device that provides connections for individual computers or other hubs and switches.

Gateways

Gateway is a general term for software running on a device that connects two different environments and that many times acts as a translator for them or somehow restricts their interactions. Usually a gateway is needed when one environment speaks a different language, meaning it uses a certain protocol that the other environment does not understand. The gateway can translate Internetwork Packet Exchange (IPX) protocol packets to IP packets, accept mail from one type of mail server and format it so another type of mail server can accept and understand it, or connect and translate different data link technologies such as FDDI to Ethernet.

Gateway Server

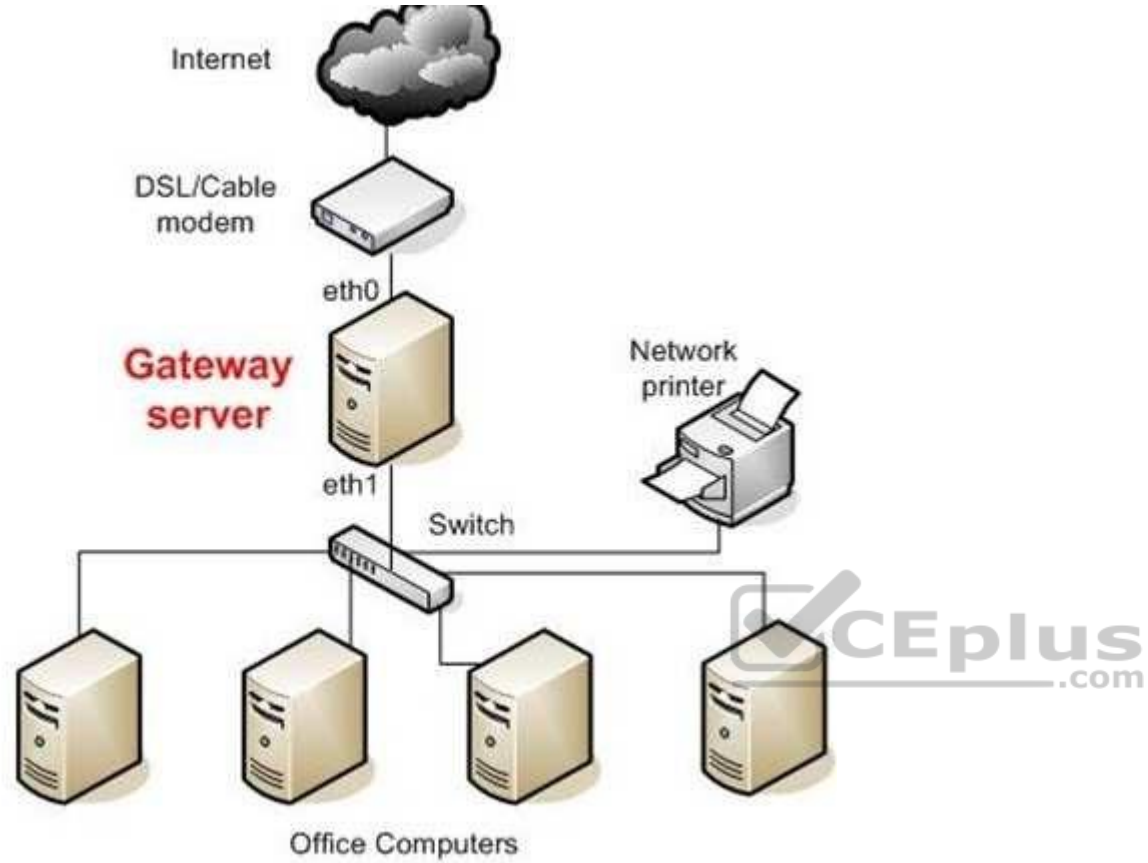


Image Reference- http://static.howtoforge.com/images/screenshots/556af08d5e43aa768260f9e589dc547f-3024.jpg

The following answers are incorrect:

Repeater - A repeater provides the simplest type of connectivity, because it only repeats electrical signals between cable segments, which enables it to extend a network. Repeaters work at the physical layer and are add-on devices for extending a network connection over a greater distance. The device amplifies signals because signals attenuate the farther they have to travel.

Bridges - A bridge is a LAN device used to connect LAN segments. It works at the data link layer and therefore works with MAC addresses. A repeater does not work with addresses; it just forwards all signals it receives. When a frame arrives at a bridge, the bridge determines whether or not the MAC address is on the local network segment. If the MAC address is not on the local network segment, the bridge forwards the frame to the necessary network segment.

Routers - Routers are layer 3, or network layer, devices that are used to connect similar or different networks. (For example, they can connect two Ethernet LANs or an Ethernet LAN to a Token Ring LAN.) A router is a device that has two or more interfaces and a routing table so it knows how to get packets to their destinations. It can filter traffic based on access control lists (ACLs), and it fragments packets when necessary.

Following reference(s) were/was used to create this question:
CISA review manual 2014 Page number 263
Official ISC2 guide to CISSP CBK 3rd Edition Page number 229 and 230

QUESTION 419
In which layer of the OSI Model are connection-oriented protocols located in the TCP/IP suite of protocols?

A. Transport layer
B. Application layer
C. Physical layerD. Network layer

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Connection-oriented protocols such as TCP provides reliability.

It is the responsibility of such protocols in the transport layer to ensure every byte is accounted for. The network layer does not provide reliability. It only privides the best route to get the traffic to the final destination address.

For your exam you should know the information below about OSI model:

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal.

OSI Model

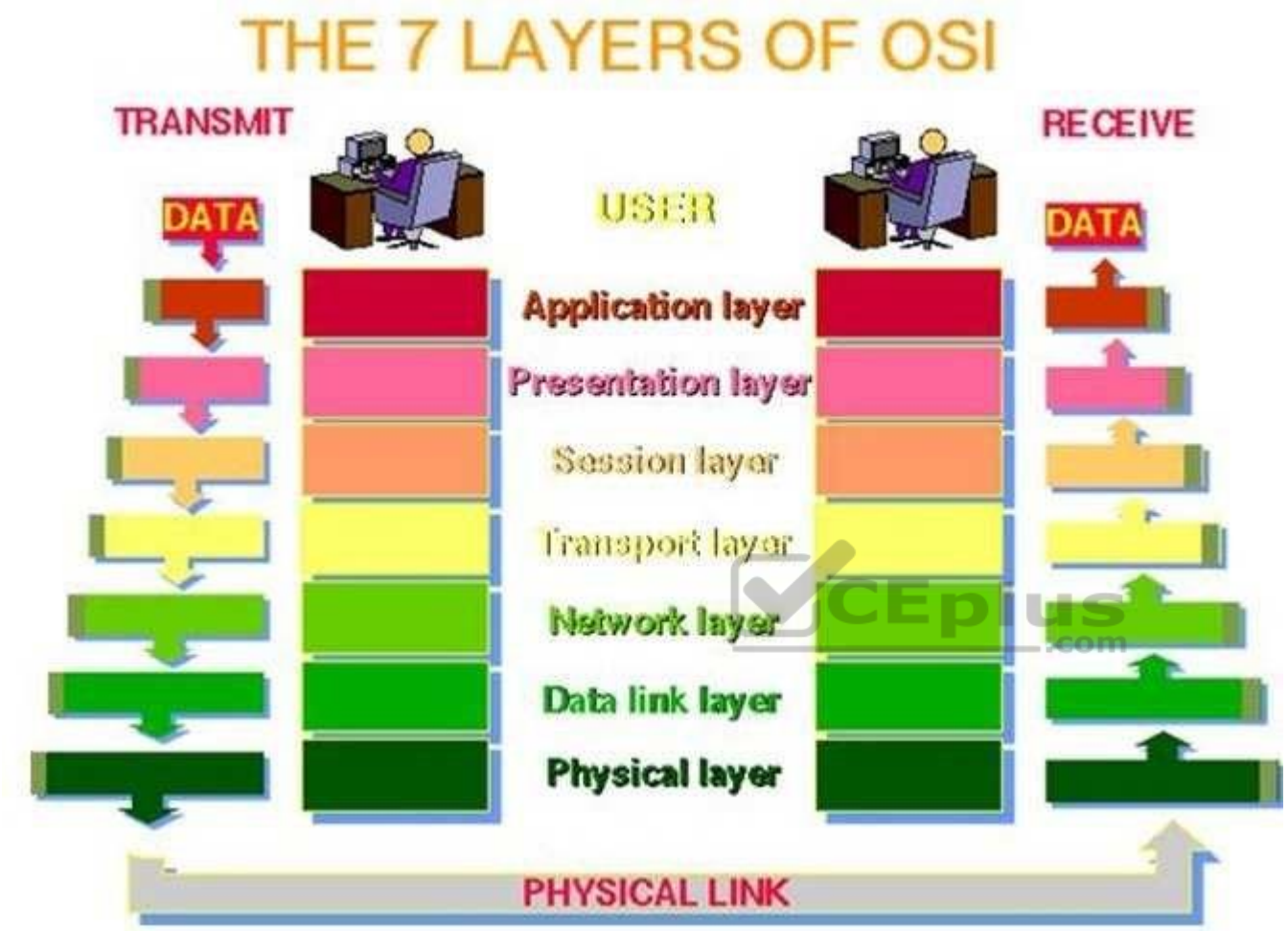


Image source: http://www.petri.co.il/images/osi_model.JPG

PHYSICAL LAYER
The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:

What signal state represents a binary 1
How the receiving station knows when a "bit-time" starts
How the receiving station delimits a frame

DATA LINK LAYER

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually errorfree transmission over the link. To do this, the data link layer provides:

Link establishment and termination: establishes and terminates the logical link between two nodes.
Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
Frame sequencing: transmits/receives frames sequentially.
Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting nonacknowledged frames and handling duplicate frame receipt.
Frame delimiting: creates and recognizes frame boundaries.
Frame error checking: checks received frames for integrity.
Media access management: determines when the node "has the right" to use the physical medium.

NETWORK LAYER

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

Routing: routes frames among networks.
Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet

The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet).

In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems.

TRANSPORT LAYER
The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers.

The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
Message acknowledgment: provides reliable end-to-end message delivery with acknowledgments.
Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers
Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

SESSION LAYER
The session layer allows session establishment between processes running on different stations. It provides:

Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.

Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

PRESENTATION LAYER

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

Character code translation: for example, ASCII to EBCDIC.
Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
Data compression: reduces the number of bits that need to be transmitted on the network.
Data encryption: encrypt data for security purposes. For example, password encryption.

APPLICATION LAYER

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

Resource sharing and device redirection
Remote file access
Remote printer access
Inter-process communication
Network management
Directory services
Electronic messaging (such as mail)
Network virtual terminals

The following were incorrect answers:

Application Layer - The application layer serves as the window for users and application processes to access network services.

Network layer - The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.

Physical Layer - The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.

The following reference(s) were/was used to create this question:

CISA review manual 2014 Page number 260
and
Official ISC2 guide to CISSP CBK 3rd Edition Page number 287
and
http://en.wikipedia.org/wiki/Tcp_protocol

QUESTION 420
Which of the following is a telecommunication device that translates data from digital to analog form and back to digital?

A. Multiplexer
B. Modem
C. Protocol converter
D. Concentrator

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A modem is a device that translates data from digital form and then back to digital for communication over analog lines.
Source: Information Systems Audit and Control Association,
Certified Information Systems Auditor 2002 review manual, Chapter 3: Technical Infrastructure and Operational Practices (page 114).

QUESTION 421
Which of the following transmission media would NOT be affected by cross talk or interference?

A. Copper cable
B. Radio System
C. Satellite radiolink
D. Fiber optic cables

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Only fiber optic cables are not affected by crosstalk or interference.

For your exam you should know the information about transmission media:

Copper Cable
Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.
Copper has been used in electric wiring since the invention of the electromagnet and the telegraph in the 1820s.The invention of the telephone in 1876 created further demand for copper wire as an electrical conductor.
Copper is the electrical conductor in many categories of electrical wiring. Copper wire is used in power generation, power transmission, power distribution, telecommunications, electronics circuitry, and countless types of electrical equipment. Copper and its alloys are also used to make electrical contacts. Electrical wiring in buildings is the most important market for the copper industry. Roughly half of all copper mined is used to manufacture electrical wire and cable conductors.

Copper Cable

Image Source - http://i00.i.aliimg.com/photo/v0/570456138/FRLS_HR_PVC_Copper_Cable.jpg

Coaxial cable

Coaxial cable, or coax (pronounced 'ko.aks), is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside, who patented the design in 1880.Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

Coaxial cable are expensive and does not support many LAN's. It supports data and video

Coaxial Cable

Image Source - http://www.tlc-direct.co.uk/Images/Products/size_3/CARG59.JPG

Fiber optics
An optical fiber cable is a cable containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed. Different types of cable are used for different applications, for example long distance telecommunication, or providing a high-speed data connection between different parts of a building.

Fiber optics used for long distance, hard to splice, not vulnerable to cross talk and difficult to tap. It supports voice data, image and video.
Radio System
Radio systems are used for short distance,cheap and easy to tap.
Radio is the radiation (wireless transmission) of electromagnetic signals through the atmosphere or free space.

Information, such as sound, is carried by systematically changing (modulating) some property of the radiated waves, such as their amplitude, frequency, phase, or pulse width. When radio waves strike an electrical conductor, the oscillating fields induce an alternating current in the conductor. The information in the waves can be extracted and transformed back into its original form.

Fiber Optics

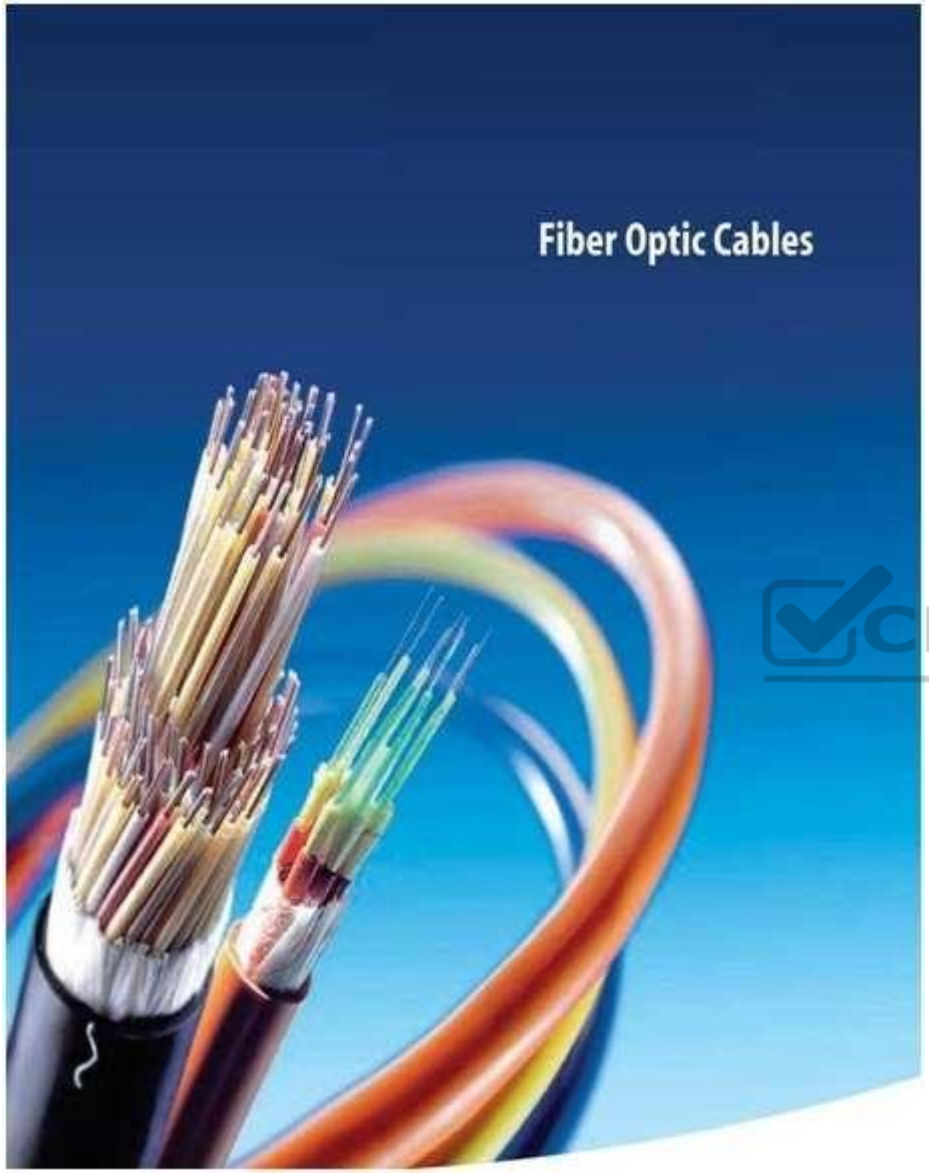


Image Source - http://aboveinfranet.com/wp-content/uploads/2014/04/fiber-optic-cables-above-infranet-solutions.jpg Microwave radio system

Microwave transmission refers to the technology of transmitting information or energy by the use of radio waves whose wavelengths are conveniently measured in small numbers of centimetre; these are called microwaves.
Microwaves are widely used for point-to-point communications because their small wavelength allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna. This allows nearby microwave equipment to use the same frequencies without interfering with each other, as lower frequency radio waves do. Another advantage is that the high frequency of microwaves gives the microwave band a very large information-carrying capacity; the microwave band has a bandwidth 30 times that of all the rest of the radio spectrum below it. A disadvantage is that microwaves are limited to line of sight propagation; they cannot pass around hills or mountains as lower frequency radio waves can.

Microwave radio transmission is commonly used in point-to-point communication systems on the surface of the Earth, in satellite communications, and in deep space radio communications. Other parts of the microwave radio band are used for radars, radio navigation systems, sensor systems, and radio astronomy.

Microwave radio systems are carriers for voice data signal, cheap and easy to tap.

Microwave Radio System

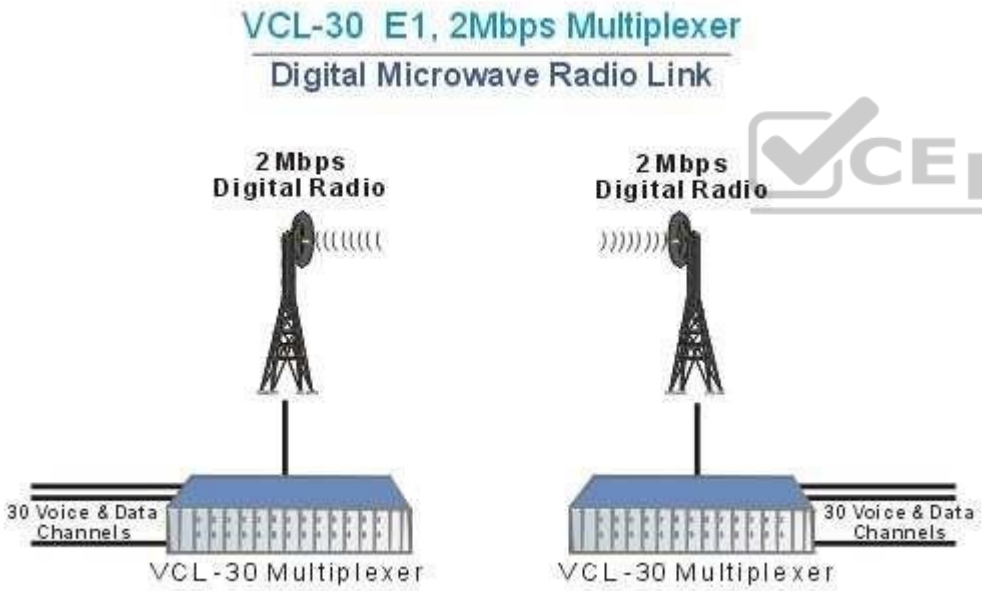


Image Source - http://www.valiantcom.com/images/applications/e1_digital_microwave_radio.gif

Satellite Radio Link

Satellite radio is a radio service broadcast from satellites primarily to cars, with the signal broadcast nationwide, across a much wider geographical area than terrestrial radio stations. It is available by subscription, mostly commercial free, and offers subscribers more stations and a wider variety of programming options than terrestrial radio.

Satellite radio link uses transponder to send information and easy to tap.

The following answers are incorrect:

Copper Cable - Copper cable is very simple to install and easy to tap. It is used mostly for short distance and supports voice and data.

Radio System - Radio systems are used for short distance,cheap and easy to tap.

Satellite Radio Link - Satellite radio link uses transponder to send information and easy to tap.

The following reference(s) were/was used to create this question:

CISA review manual 2014 page number 265 &
Official ISC2 guide to CISSP CBK 3rd Edition Page number 233

QUESTION 422
What is called an attack where the attacker spoofs the source IP address in an ICMP ECHO broadcast packet so it seems to have originated at the victim's system, in order to flood it with REPLY packets?

A. SYN Flood attack
B. Smurf attack
C. Ping of Death attack
D. Denial of Service (DOS) attack

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Although it may cause a denial of service to the victim's system, this type of attack is a Smurf attack. A SYN Flood attack uses up all of a system's resources by setting up a number of bogus communication sockets on the victim's system. A Ping of Death attack is done by sending IP packets that exceed the maximum legal length (65535 octets).
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 789).

QUESTION 423

What is the main difference between a Smurf and a Fraggle attack?

A. A Smurf attack is ICMP-based and a Fraggle attack is UDP-based.
B. A Smurf attack is UDP-based and a Fraggle attack is TCP-based.
C. Smurf attack packets cannot be spoofed.
D. A Smurf attack is UDP-based and a Fraggle attack is ICMP-based.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Fraggle is an attack similar to Smurf, but instead of using ICMP, it uses UDP.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 11: Application and System Development (page 790).

QUESTION 424
Why are coaxial cables called "coaxial"?

A. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.
B. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis
C. it includes two physical channels that carries the signal surrounded (after a layer of insulation) by another two concentric physical channels, both running along the same axis.
D. it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running perpendicular and along the different axis

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis.

The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance.

Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 14.

QUESTION 425
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers does NOT have which of the following characteristics?

A. Standard model for network communications
B. Used to gain information from network devices such as count of packets received and routing tables
C. Enables dissimilar networks to communicate
D. Defines 7 protocol layers (a.k.a. protocol stack)

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The International Standards Organization / Open Systems Interconnection (ISO/OSI) Layers and Characteristics Standard model for network communications enables dissimilar networks to communicate, Defines 7 protocol layers (a.k.a. protocol stack) Each layer on one workstation communicates with its respective layer on another workstation using protocols (i.e. agreed-upon communication formats) "Mapping" each protocol to the model is useful for comparing protocols.
Mnemonics: Please Do Not Throw Sausage Pizza Away (bottom to top layer) All People Seem To Need Data Processing (top to bottom layer).
Source: STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 12.

QUESTION 426
In telephony different types of connections are being used. The connection from the phone company's branch office to local customers is referred to as which of the following choices?

A. new loop
B. local loop
C. loopback
D. indigenous loop

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Transmission on fiber optic wire requires repeating at distance intervals. The glass fiber requires more protection within an outer cable than copper. For these reasons and because the installation of any new wiring is labor-intensive, few communities yet have fiber optic wires or cables from the phone company's branch office to local customers (local loop).

In telephony, a local loop is the wired connection from a telephone company's central office in a locality to its customers' telephones at homes and businesses. This connection is usually on a pair of copper wires called twisted pair. The system was originally designed for voice transmission only using analog transmission technology on a single voice channel. Today, your computer's modem makes the conversion between analog signals and digital signals. With Integrated Services Digital Network (ISDN) or Digital Subscriber Line (DSL), the local loop can carry digital signals directly and at a much higher bandwidth than they do for voice only.

Local Loop diagram

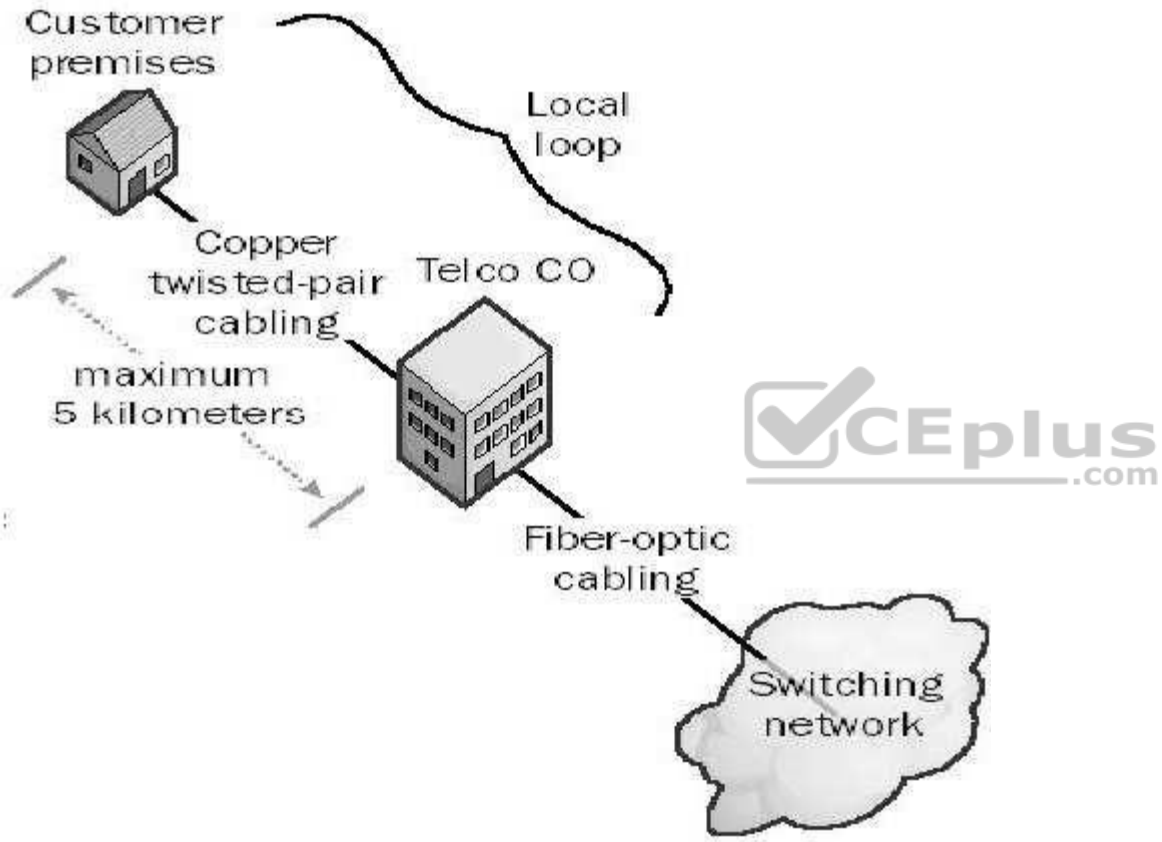


Image from: http://www.thenetworkencyclopedia.com/entry/local-loop/

The following are incorrect answers:

New loop This is only a detractor and does not exist

Loopback In telephone systems, a loopback is a test signal sent to a network destination that is returned as received to the originator. The returned signal may help diagnose a problem.

Ingenious loop This is only a detractor and does not exist

Reference(s) used for this question:
http://searchnetworking.techtarget.com/definition/local-loop
and
STEINER, Kurt, Telecommunications and Network Security, Version 1, May 2002, CISSP Open Study Group (Domain Leader: skottikus), Page 14.

QUESTION 427
Communications and network security relates to transmission of which of the following?

A. voice
B. voice and multimedia
C. data and multimedia
D. voice, data and multimedia

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
From the published (ISC)2 goals for the Certified Information Systems Security Professional candidate:

The CISSP candidate should be familiar to communications and network security as it relates to voice, data, multimedia, and facsimile transmissions in terms of local area, wide area, and remote access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 57.

QUESTION 428
One of the following statements about the differences between PPTP and L2TP is NOT true

A. PPTP can run only on top of IP networks.
B. PPTP is an encryption protocol and L2TP is not.
C. L2TP works well with all firewalls and network devices that perform NAT.
D. L2TP supports AAA servers

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
L2TP is affected by packet header modification and cannot cope with firewalls and network devices that perform NAT.

"PPTP can run only on top of IP networks." is correct as PPTP encapsulates datagrams into an IP packet, allowing PPTP to route many network protocols across an IP network.

"PPTP is an encryption protocol and L2TP is not." is correct. When using PPTP, the PPP payload is encrypted with Microsoft Point-to-Point Encryption (MPPE) using MSCHAP or EAP-TLS.

"L2TP supports AAA servers" is correct as L2TP supports TACACS+ and RADIUS.

NOTE:
L2TP does work over NAT. It is possible to use a tunneled mode that wraps every packet into a UDP packet. Port 4500 is used for this purpose. However this is not true of PPTP and it is not true as well that it works well with all firewalls and NAT devices.

References:
All in One Third Edition page 545
Official Guide to the CISSP Exam page 124-126

QUESTION 429
You have been tasked to develop an effective information classification program. Which one of the following steps should be performed first?

A. Establish procedures for periodically reviewing the classification and ownership
B. Specify the security controls required for each classification level
C. Identify the data custodian who will be responsible for maintaining the security level of data
D. Specify the criteria that will determine how data is classified

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
According to the AIO 3rd edition, these are the necessary steps for a proper classification program:
1. Define classification levels.
2. Specify the criteria that will determine how data is classified.

3. Have the data owner indicate the classification of the data she is responsible for.
4. Identify the data custodian who will be responsible for maintaining data and its security level.
5. Indicate the security controls, or protection mechanisms, that are required for each classification level.
6. Document any exceptions to the previous classification issues.
7. Indicate the methods that can be used to transfer custody of the information to a different data owner.
8. Create a procedure to periodically review the classification and ownership. Communicate any changes to the data custodian.
9. Indicate termination procedures for declassifying the data.
10. Integrate these issues into the security-awareness program so that all employees understand how to handle data at different classification levels.

Domain: Information security and risk management

Reference: AIO 3rd edition page 50

QUESTION 430
A group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability is:

A. server cluster
B. client cluster
C. guest cluster
D. host cluster

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A server cluster is a group of independent servers, which are managed as a single system, that provides higher availability, easier manageability, and greater scalability.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 431
A server cluster looks like a:

A. single server from the user's point of view
B. dual server from the user's point of view
C. triple server from the user's point of view
D. quardle server from the user's point of view

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The cluster looks like a single server from the user's point of view.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 432
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a:

A. server farm
B. client farm
C. cluster farm
D. host farm

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
If any server in the cluster crashes, processing continues transparently, however, the cluster suffers some performance degradation. This implementation is sometimes called a "server farm."
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 67.

QUESTION 433
Which of the following is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length?

A. Fiber Optic cable
B. Coaxial cable
C. Twisted Pair cable
D. Axial cable

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Fiber Optic cable is immune to the effects of electromagnetic interference (EMI) and therefore has a much longer effective usable length (up to two kilometers in some cases).
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 72.

QUESTION 434
Which of the following methods of providing telecommunications continuity involves the use of an alternative media?

A. Alternative routing
B. Diverse routing
C. Long haul network diversity
D. Last mile circuit protection

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits or end points should the normal network be unavailable. Diverse routing routes traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and therefore subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual entrance facilities. This type of access is time-consuming and costly. Long haul network diversity is a diverse long-distance network utilizing T1 circuits among the major long-distance carriers. It ensures long-distance access should any one carrier experience a network failure. Last mile circuit protection is a redundant combination of local carrier T1s microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also utilized.
Source: Information Systems Audit and Control Association, Certified Information Systems Auditor 2002 review manual, chapter 5: Disaster Recovery and Business Continuity (page 259).

QUESTION 435
Which port does the Post Office Protocol Version 3 (POP3) make use of?

A. 110
B. 109
C. 139
D. 119

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The other answers are not correct because of the following protocol/port numbers matrix:

Post Office Protocol (POP2) 109
Network News Transfer Protocol 119
NetBIOS 139

QUESTION 436
Which of the following are WELL KNOWN PORTS assigned by the IANA?

A. Ports 0 to 255
B. Ports 0 to 1024
C. Ports 0 to 1023
D. Ports 0 to 127

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The port numbers are divided into three ranges: the Well Known Ports, the Registered Ports, and the Dynamic and/or Private Ports. The range for assigned "Well Known" ports managed by the IANA (Internet Assigned Numbers Authority) is 0-1023.

Source: iana.org: port assignments.

QUESTION 437
Which of the following are REGISTERED PORTS as defined by IANA ?

A. Ports 128 to 255
B. Ports 1024 to 49151C. Ports 1025 to 65535
D. Ports 1024 to 32767

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Ports 1024 to 49151 has been defined as REGISTERED PORTS by IANA.

A registered port is a network port (a sub-address defined within the Internet Protocol, in the range 1–65535) assigned by the Internet Assigned Numbers Authority (IANA) (or by Internet Corporation for Assigned Names and Numbers (ICANN) before March 21, 2001) for use with a certain protocol or application.

Ports with numbers lower than those of the registered ports are called well known ports; ports with numbers greater than those of the registered ports are called dynamic and/or private ports.

Ports 0-1023 - well known ports
Ports 1024-49151 - Registered port: vendors use for applications
Ports >49151 - dynamic / private ports

The other answers are not correct

Reference(s) used for this question:
http://en.wikipedia.org/wiki/Registered_port

QUESTION 438

Which of the following countermeasures would be the most appropriate to prevent possible intrusion or damage from wardialing attacks?

A. Monitoring and auditing for such activity
B. Require user authentication
C. Making sure only necessary phone numbers are made public
D. Using completely different numbers for voice and data accesses

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Knowlege of modem numbers is a poor access control method as an attacker can discover modem numbers by dialing all numbers in a range. Requiring user authentication before remote access is granted will help in avoiding unauthorized access over a modem line.

"Monitoring and auditing for such activity" is incorrect. While monitoring and auditing can assist in detecting a wardialing attack, they do not defend against a successful wardialing attack.

"Making sure that only necessary phone numbers are made public" is incorrect. Since a wardialing attack blindly calls all numbers in a range, whether certain numbers in the range are public or not is irrelevant.

"Using completely different numbers for voice and data accesses" is incorrect. Using different number ranges for voice and data access might help prevent an attacker from stumbling across the data lines while wardialing the public voice number range but this is not an adequate countermeaure.

References:
CBK, p. 214

AIO3, p. 534-535

QUESTION 439
What is the maximum length of cable that can be used for a twisted-pair, Category 5 10Base-T cable?

A. 80 meters
B. 100 metersC. 185 meters
D. 500 meters

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
As a signal travels though a medium, it attenuates (loses strength) and at some point will become indistinguishable from noise. To assure trouble-free communication, maximum cable lengths are set between nodes to assure that attenuation will not cause a problem. The maximum CAT-5 UTP cable length between two nodes for 10BASE-T is 100M.

The following answers are incorrect:

80 meters. It is only a distracter.
185 meters. Is incorrect because it is the maximum length for 10Base-2
500 meters. Is incorrect because it is the maximum length for 10Base-5

QUESTION 440
What type of cable is used with 100Base-TX Fast Ethernet?

A. Fiber-optic cable
B. Category 3 or 4 unshielded twisted-pair (UTP).
C. Category 5 unshielded twisted-pair (UTP).
D. RG-58 cable.

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
This is the type of cabling recommended for 100Base-TX networks.

Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling.

"Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for 100Mbps operation.

RG-58 cable is incorrect. Incorrect media type for 100Base-TX.

References
CBK, p. 428
AIO3, p. 455

QUESTION 441
Secure Sockets Layer (SSL) is very heavily used for protecting which of the following?

A. Web transactions.
B. EDI transactions.
C. Telnet transactions.
D. Electronic Payment transactions.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
SSL was developed Netscape Communications Corporation to improve security and privacy of HTTP transactions.

SSL is one of the most common protocols used to protect Internet traffic.
It encrypts the messages using symmetric algorithms, such as IDEA, DES, 3DES, and Fortezza, and also calculates the MAC for the message using MD5 or SHA1. The MAC is appended to the message and encrypted along with the message data.

The exchange of the symmetric keys is accomplished through various versions of Diffie–Hellmann or RSA. TLS is the Internet standard based on SSLv3. TLSv1 is backward compatible with SSLv3. It uses the same algorithms as SSLv3; however, it computes an HMAC instead of a MAC along with other enhancements to improve security.

The following are incorrect answers:

"EDI transactions" is incorrect. Electronic Data Interchange (EDI) is not the best answer to this question though SSL could play a part in some EDI transactions.

"Telnet transactions" is incorrect. Telnet is a character mode protocol and is more likely to be secured by Secure Telnet or replaced by the Secure Shell (SSH) protocols.

"Eletronic payment transactions" is incorrect. Electronic payment is not the best answer to this question though SSL could play a part in some electronic payment transactions.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 16615-16619). Auerbach Publications. Kindle Edition. and
http://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 442
Secure Shell (SSH) is a strong method of performing:

A. client authentication
B. server authentication
C. host authentication
D. guest authentication

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Secure shell (SSH) was designed as an alternative to some of the insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.

SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel.

The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates.

Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.

There are two incompatible versions of the protocol, SSH-1 and SSH-2, though many servers support both. SSH-2 has improved integrity checks (SSH-1 is vulnerable to an insertion attack due to weak CRC-32 integrity checking) and supports local extensions and additional types of digital certificates such as Open PGP. SSH was originally designed for UNIX, but there are now implementations for other operating systems, including Windows, Macintosh, and OpenVMS.

Is SSH 3.0 the same as SSH3?
The short answer is: NO SSH 3.0 refers to version 3 of SSH Communications SSH2 protocol implementation and it could also refer to OpenSSH Version 3.0 of its SSH2 software. The "3" refers to the software release version not the protocol version. As of this writing (July 2013), there is no SSH3 protocol.

"Server authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.

"Host authentication" is incorrect. Though many SSH clients allow pre-caching of server/host keys, this is a minimal form of server/host authentication.

"Guest authentication" is incorrect. The general idea of "guest" is that it is unauthenticated access.

Reference(s) used for this question:

http://www.ietf.org/rfc/rfc4252.txt
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7080-7088). Auerbach Publications. Kindle Edition.

QUESTION 443
Secure Shell (SSH-2) supports authentication, compression, confidentiality, and integrity, SSH is commonly used as a secure alternative to all of the following protocols below except:

A. telnet
B. rlogin
C. RSH
D. HTTPS

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
HTTPS is used for secure web transactions and is not commonly replaced by SSH.

Users often want to log on to a remote computer. Unfortunately, most early implementations to meet that need were designed for a trusted network. Protocols/ programs, such as TELNET, RSH, and rlogin, transmit unencrypted over the network, which allows traffic to be easily intercepted. Secure shell (SSH) was designed as an alternative to the above insecure protocols and allows users to securely access resources on remote computers over an encrypted tunnel. SSH's services include remote log-on, file transfer, and command execution. It also supports port forwarding, which redirects other protocols through an encrypted SSH tunnel. Many users protect less secure traffic of protocols, such as X Windows and VNC (virtual network computing), by forwarding them through a SSH tunnel. The SSH tunnel protects the integrity of communication, preventing session hijacking and other man-in-the-middle attacks. Another advantage of SSH over its predecessors is that it supports strong authentication. There are several alternatives for SSH clients to authenticate to a SSH server, including passwords and digital certificates. Keep in mind that authenticating with a password is still a significant improvement over the other protocols because the password is transmitted encrypted.

The following were wrong answers:

telnet is an incorrect choice. SSH is commonly used as an more secure alternative to telnet. In fact Telnet should not longer be used today. rlogin is and incorrect choice. SSH is commonly used as a more secure alternative to rlogin. RSH is an incorrect choice. SSH is commonly used as a more secure alternative to RSH.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7077-7088). Auerbach Publications. Kindle Edition.

QUESTION 444
Secure Shell (SSH-2) provides all the following services except:

A. secure remote login
B. command execution
C. port forwarding
D. user authentication

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
This is one of the tricky negative question. You have to pay close attention to the word EXCEPT within the question.

The SSH transport layer is a secure, low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.

Authentication in this protocol level is host-based; this protocol does not perform user authentication. A higher level protocol for user authentication can be designed on top of this protocol.

The protocol has been designed to be simple and flexible to allow parameter negotiation, and to minimize the number of round-trips. The key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated. It is expected that in most environments, only 2 round-trips will be needed for full key exchange, server authentication, service request, and acceptance notification of service request. The worst case is 3 round-trips.

The following are incorrect answers:

"Remote log-on" is incorrect. SSH does provide remote log-on.
"Command execution" is incorrect. SSH does provide command execution.

"Port forwarding" is incorrect. SSH does provide port forwarding. SSH also has a wonderful feature called SSH Port Forwarding, sometimes called SSH Tunneling, which allows you to establish a secure SSH session and then tunnel arbitrary TCP connections through it. Tunnels can be created at any time, with almost no effort and no programming, which makes them very appealing. See the article below in the reference to take a look at SSH Port Forwarding in detail, as it is a very useful but often misunderstood technology. SSH Port Forwarding can be used for secure communications in a myriad of different ways.

You can see a nice tutorial on the PUTTY web site on how to use PUTTY to do port forwarding at:
http://www.cs.uu.nl/technical/services/ssh/putty/puttyfw.html

Reference(s) used for this question:
RFC 4253 at https://www.ietf.org/rfc/rfc4253.txt
and
SSH Port Forwarding by Symantec

QUESTION 445
Transport Layer Security (TLS) is a two-layered socket layer security protocol that contains the TLS Record Protocol and the::

A. Transport Layer Security (TLS) Internet Protocol.
B. Transport Layer Security (TLS) Data Protocol.
C. Transport Layer Security (TLS) Link Protocol.
D. Transport Layer Security (TLS) Handshake Protocol.

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:

QUESTION 446
Similar to Secure Shell (SSH-2), Secure Sockets Layer (SSL) uses symmetric encryption for encrypting the bulk of the data being sent over the session and it uses asymmetric or public key cryptography for:

A. Peer Authentication
B. Peer Identification
C. Server Authentication
D. Name Resolution

Correct Answer: A
Section: Network and Telecommunications
Explanation
Explanation/Reference:

SSL provides for Peer Authentication. Though peer authentication is possible, authentication of the client is seldom used in practice when connecting to public ecommerce web sites. Once authentication is complete, confidentiality is assured over the session by the use of symmetric encryption in the interests of better performance.

The following answers were all incorrect:

"Peer identification" is incorrect. The desired attribute is assurance of the identity of the communicating parties provided by authentication and NOT identification. Identification is only who you claim to be. Authentication is proving who you claim to be.

"Server authentication" is incorrect. While server authentication only is common practice, the protocol provides for peer authentication (i.e., authentication of both client and server). This answer was not complete.

"Name resolution" is incorrect. Name resolution is commonly provided by the Domain Name System (DNS) not SSL.

Reference(s) used for this question:
CBK, pp. 496 - 497.

QUESTION 447
What can a packet filtering firewall also be called?

A. a scanning router
B. a shielding router
C. a sniffing router
D. a screening router

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
While neither CBK nor AIO3 use the term "screening router," they both discuss how the packet filtering capabilities of a router can be used to block traffic much like a packet filtering firewall. Krutz and Vine use this term on p. 90.

"A scanning router" is incorrect. This is a nonsense term to distract you.
"A shielding router" is incorrect. This is a nonsense term to distract you.
"A sniffing router" is incorrect. This is a nonsense term to distract you.

References:
CBK, p. 433

AIO3, pp.484 - 485

QUESTION 448
Packet Filtering Firewalls examines both the source and destination address of the:

A. incoming and outgoing data packets
B. outgoing data packets only
C. Incoming Data packets only
D. user data packet

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Packeting filtering firewalls are devices that enforce administrative security policies by filtering incoming traffic as well as outgoing traffic based on rules that can include the source and/or destination addresses.

"Outgoing data packets" is incorrect. Firewalls filter incoming as well as outgoing traffic. This is sometimes called Egress and Ingress filtering.

"Incoming data packets only" is incorrect. (see previous explantion)

"User data packet" is incorrect. A packet filtering firewall does not typicallly look into the data portion of the packet.

References
CBK, p. 464
AIO3, pp. 482 - 484

QUESTION 449
Packet Filtering Firewalls can also enable access for:

A. only authorized application port or service numbers.
B. only unauthorized application port or service numbers.
C. only authorized application port or ex-service numbers.
D. only authorized application port or service integers.

Correct Answer: A

Section: Network and Telecommunications
Explanation
Explanation/Reference:
Firewall rules can be used to enable access for traffic to specific ports or services. "Service numbers" is rather stilted English but you may encounter these types of wordings on the actual exam -- don't let them confuse you.

"Only unauthorized application port or service numbers" is incorrect. Unauthorized ports/services would be blocked in a properly installed firewall rather than permitting access.

"Only authorized application port or ex-service numbers" is incorrect. "Ex-service" numbers is a nonsense term meant to distract you.

"Only authorized application port or service integers." While service numbers are in fact integers, the more usual (and therefore better) answer is either service or "service number."

References
CBK, p. 464
AIO3, pp. 482 – 484

QUESTION 450
A Packet Filtering Firewall system is considered a:

A. first generation firewall.
B. second generation firewall.
C. third generation firewall.
D. fourth generation firewall.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The first types of firewalls were packet filtering firewalls. It is the most basic firewall making access decisions based on ACL's. It will filter traffic based on source IP and port as well as destination IP and port. It does not understand the context of the communication and inspects every single packet one by one without understanding the context of the connection.

"Second generation firewall" is incorrect. The second generation of firewall were Proxy based firewalls. Under proxy based firewall you have Application Level Proxy and also the Circuit-level proxy firewall. The application level proxy is very smart and understand the inner structure of the protocol itself. The Circui-Level Proxy is a generic proxy that allow you to proxy protocols for which you do not have an Application Level Proxy. This is better than allowing a direct connection to the net. Today a great example of this would be the SOCKS protocol.

"Third generation firewall" is incorrect. The third generation firewall is the Stateful Inspection firewall. This type of firewall makes use of a state table to maintain the context of connections being established.

"Fourth generation firewall" is incorrect. The fourth generation firewall is the dynamic packet filtering firewall.

References:
CBK, p. 464
AIO3, pp. 482 - 484

Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

QUESTION 451
Proxies works by transferring a copy of each accepted data packet from one network to another, thereby masking the:

A. data's payload
B. data's details
C. data's owner
D. data's origin

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The application firewall (proxy) relays the traffic from a trusted host running a specific application to an untrusted server. It will appear to the untrusted server as if the request originated from the proxy server.

"Data's payload" is incorrect. Only the origin is changed.
"Data's details" is incorrect. Only the origin is changed.
"Data's owner" is incorrect. Only the origin is changed.

References:
CBK, p. 467
AIO3, pp. 486 - 490

QUESTION 452
A proxy can control which services (FTP and so on) are used by a workstation , and also aids in protecting the network from outsiders who may be trying to get information about the:

A. network's design
B. user base
C. operating system design

D. net BIOS' design

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
To the untrusted host, all traffic seems to originate from the proxy server and addresses on the trusted network are not revealed.

"User base" is incorrect. The proxy hides the origin of the request from the untrusted host.

"Operating system design" is incorrect. The proxy hides the origin of the request from the untrusted host.

"Net BIOS' design" is incorrect. The proxy hides the origin of the request from the untrusted host.

References:
CBK, p. 467
AIO3, pp. 486 - 490

QUESTION 453
A proxy is considered a:

A. first generation firewall.
B. third generation firewall.
C. second generation firewall.
D. fourth generation firewall.

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The proxy (application layer firewall, circuit level proxy, or application proxy) is a second generation firewall

"First generation firewall" incorrect. A packet filtering firewall is a first generation firewall.

"Third generation firewall" is incorrect. Stateful Firewall are considered third generation firewalls
"Fourth generation firewall" is incorrect. Dynamic packet filtering firewalls are fourth generation firewalls

References:
CBK, p. 464
AIO3, pp. 482 - 484

Neither CBK or AIO3 use the generation terminology for firewall types but you will encounter it frequently as a practicing security professional. See http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm for a general discussion of the different generations.

QUESTION 454
An application layer firewall is also called a:

A. Proxy
B. A Presentation Layer Gateway.
C. A Session Layer Gateway.
D. A Transport Layer Gateway.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
An application layer firewall can also be called a proxy.

"A presentation layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.

"A session layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.

"A transport layer gateway" is incorrect. A gateway connects two unlike environments and is usually required to translate between diffferent types of applications or protocols. This is not the function of a firewall.

References:
CBK, p. 467
AIO3, pp. 486 - 490, 960

QUESTION 455
Application Layer Firewalls operate at the:

A. OSI protocol Layer seven, the Application Layer.
B. OSI protocol Layer six, the Presentation Layer.
C. OSI protocol Layer five, the Session Layer.
D. OSI protocol Layer four, the Transport Layer.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Since the application layer firewall makes decisions based on application-layer information in the packet, it operates at the application layer of the OSI stack.

"OSI protocol layer 6, the presentation layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.

"OSI protocol layer 5, the session layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.

"OSI protocol layer 4, the transport layer" is incorrect. The application layer firewall must have access to the application layer information in the packet and therefore operates at the application layer.

References:
CBK, p. 467
AIO3, pp.488 - 490

QUESTION 456
A variation of the application layer firewall is called a:

A. Current Level Firewall.
B. Cache Level Firewall.
C. Session Level Firewall.
D. Circuit Level Firewall.

Correct Answer: D

Section: Network and Telecommunications
Explanation

Explanation/Reference:
Terminology can be confusing between the different souces as both CBK and AIO3 call an application layer firewall a proxy and proxy servers are generally classified as either circuit-level proxies or application level proxies.

The distinction is that a circuit level proxy creates a conduit through which a trusted host can communicate with an untrusted one and doesn't really look at the application contents of the packet (as an application level proxy does). SOCKS is one of the better known circuit-level proxies.

Firewalls
Packet Filtering Firewall - First Generation

n Screening Router n Operates at Network and

Transport level n Examines Source and

Destination IP Address n Can deny based on

ACLs

n Can specify Port
Application Level Firewall - Second Generation n Proxy Server n Copies each packet from one

network to the other n Masks the origin of the data n Operates at layer 7 (Application Layer) n

Reduces Network performance since it has do analyze each packet and decide what to do with it.

n Also Called Application Layer Gateway

Stateful Inspection Firewalls – Third

Generation n Packets Analyzed at all OSI

layers n Queued at the network level

n Faster than Application level Gateway
Dynamic Packet Filtering Firewalls – Fourth

Generation n Allows modification of security rules n

Mostly used for UDP

n Remembers all of the UDP packets that have crossed the network's perimeter, and it decides whether to enable packets to pass through the firewall.

Kernel Proxy – Fifth Generation n Runs in NT Kernel n Uses dynamic and custom TCP/IP-based stacks to inspect the network packets and to enforce security policies.

"Current level firewall" is incorrect. This is an amost-right-sounding distractor to confuse the unwary.

"Cache level firewall" is incorrect. This too is a distractor.

"Session level firewall" is incorrect. This too is a distractor.

References
CBK, p. 466 - 467
AIO3, pp. 486 - 490
CISSP Study Notes from Exam Prep Guide

QUESTION 457
A circuit level proxy is _____ when compared to an application level proxy.

A. lower in processing overhead.
B. more difficult to maintain.
C. more secure.
D. slower.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Since the circuit level proxy does not anayze the application content of the packet in making its decisions, it has lower overhead than an application level proxy.

"More difficult to maintain" is incorrect. Circuit level proxies are typicall easier to configure and simpler to maintain that an application level proxy.

"More secure" is incorrect. A circuit level proxy is not necessarily more secure than an application layer proxy.

"Slower" is incorrect. Because it is lower in overhead, a circuit level proxy is typically faster than an application level proxy.

References:
CBK,pp. 466 - 467
AIO3, pp.488 - 490

QUESTION 458
In a stateful inspection firewall, data packets are captured by an inspection engine that is operating at the:

A. Network or Transport Layer.

B. Application Layer.
C. Inspection Layer.
D. Data Link Layer.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Most stateful packet inspection firewalls work at the network or transport layers. For the TCP/IP protcol, this allows the firewall to make decisions both on IP addresses, protocols and TCP/UDP port numbers

Application layer is incorrect. This is too high in the OSI stack for this type of firewall.

Inspection layer is incorrect. There is no such layer in the OSI stack.

"Data link layer" is incorrect. This is too low in the OSI stack for this type of firewall.

References:
CBK, p. 466
AIO3, pp. 485 - 486

QUESTION 459
In stateful inspection firewalls, packets are:

A. Inspected at only one layer of the Open System Interconnection (OSI) model
B. Inspected at all Open System Interconnection (OSI) layers C. Decapsulated at all Open Systems Interconnect (OSI) layers.
D. Encapsulated at all Open Systems Interconnect (OSI) layers.

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Many times when a connection is opened, the firewall will inspect all layers of the packet. While this inspection is scaled back for subsequent packets to improve performance, this is the best of the four answers.

When packet filtering is used, a packet arrives at the firewall, and it runs through its ACLs to determine whether this packet should be allowed or denied. If the packet is allowed, it is passed on to the destination host, or to another network device, and the packet filtering device forgets about the packet. This is different from stateful inspection, which remembers and keeps track of what packets went where until each particular connection is closed. A stateful firewall is like a nosy neighbor who gets into people's business and conversations. She keeps track of the suspicious cars that come into the neighborhood, who is out of town for the week, and the postman who stays a little too long at the neighbor lady's house. This can be annoying until your house is burglarized. Then you and the police will want to talk to the nosy neighbor, because she knows everything going on in the neighborhood and would be the one most likely to know something unusual happened.

"Inspected at only one Open Systems Interconnetion (OSI) layer" is incorrect. To perform stateful packet inspection, the firewall must consider at least the network and transport layers.

"Decapsulated at all Open Systems Interconnection (OSI) layers" is incorrect. The headers are not stripped ("decapsulated" if there is such a word) and are passed through in their entirety IF the packet is passed.

"Encapsulated at all Open Systems Interconnect (OSI) layers" is incorrect. Encapsulation refers to the adding of a layer's header/trailer to the information received from the above level. This is done when the packet is assembled not at the firewall.

Reference(s) used for this question:
CBK, p. 466
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (pp. 632-633). McGraw-Hill. Kindle Edition.

QUESTION 460
Which OSI/ISO layer is the Media Access Control (MAC) sublayer part of?

A. Transport layer
B. Network layer
C. Data link layer
D. Physical layer

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The data link layer contains the Logical Link Control sublayer and the Media Access Control (MAC) sublayer.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 83).

QUESTION 461
How many layers are defined within the US Department of Defense (DoD) TCP/IP Model?

A. 7

B. 5 C. 4
D. 3

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The TCP/IP protocol model is similar to the OSI model but it defines only four layers:

Application
Host-to-host
Internet
Network access

Reference(s) used for this question:
http://www.novell.com/documentation/nw65/ntwk_ipv4_nw/data/hozdx4oj.html
and
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 84). also see:
http://en.wikipedia.org/wiki/Internet_Protocol_Suite#Layer_names_and_number_of_layers_in_the_literature

QUESTION 462
Which OSI/ISO layer does a SOCKS server operate at?

A. Session layer
B. Transport layer
C. Network layer
D. Data link layer

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A SOCKS based server operates at the Session layer of the OSI model.

SOCKS is an Internet protocol that allows client-server applications to transparently use the services of a network firewall. SOCKS is an abbreviation for "SOCKetS". As of Version 5 of SOCK, both UDP and TCP is supported.

One of the best known circuit-level proxies is SOCKS proxy server. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server, without requiring direct “IP-reachability”

The protocol was originally developed by David Koblas, a system administrator of MIPS Computer Systems. After MIPS was taken over by Silicon Graphics in 1992,
Koblas presented a paper on SOCKS at that year's Usenix Security Symposium and SOCKS became publicly available. The protocol was extended to version 4 by Ying-Da Lee of NEC.

SOCKS includes two components, the SOCKS server and the SOCKS client.

The SOCKS protocol performs four functions:

- Making connection requests
- Setting up proxy circuits
- Relaying application data
- Performing user authentication (optional)

Source:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96).
and
http://en.wikipedia.org/wiki/SOCKS
and
http://www.faqs.org/rfcs/rfc1928.html
and
The ISC2 OIG on page 619

QUESTION 463
Which IPSec operational mode encrypts the entire data packet (including header and data) into an IPSec packet?

A. Authentication mode
B. Tunnel mode
C. Transport modeD. Safe mode

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
In tunnel mode, the entire packet is encrypted and encased into an IPSec packet.

In transport mode, only the datagram (payload) is encrypted, leaving the IP address visible within the IP header.

Authentication mode and safe mode are not defined IPSec operational modes.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 96).

QUESTION 464
Which of the following category of UTP cables is specified to be able to handle gigabit Ethernet (1 Gbps) according to the EIA/TIA-568-B standards?

A. Category 5e UTP
B. Category 2 UTP
C. Category 3 UTP
D. Category 1e UTP

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Categories 1 through 6 are based on the EIA/TIA-568-B standards.

On the newer wiring for LANs is CAT5e, an improved version of CAT5 which used to be outside of the standard, for more information on twisted pair, please see: twisted pair.

Category	Cable Type	Mhz	Usage Speed

==========

CAT1	UTP		Analog voice, Plain Old Telephone System (POTS)
CAT2	UTP		4 Mbps on Token Ring, also used on Arcnet networks
CAT3	UTP, ScTP, STP	16 MHz	10 Mbps
CAT4	UTP, ScTP, STP	20 MHz	16 Mbps on Token Ring Networks
CAT5	UTP, ScTP, STP	100 MHz	100 Mbps on ethernet, 155 Mbps on ATM
CAT5e	UTP, ScTP, STP	100 MHz	1 Gbps (out of standard version, improved version of CAT5)
CAT6	UTP, ScTP, STP	250 MHz	10 Gbps
CAT7	ScTP, STP		600 M 100 Gbps

Category 6 has a minumum of 250 MHz of bandwidth. Allowing 10/100/1000 use with up to 100 meter cable length, along with 10GbE over shorter distances.

Category 6a or Augmented Category 6 has a minimum of 500 MHz of bandwidth. It is the newest standard and allows up to 10GbE with a length up to 100m.

Category 7 is a future cabling standard that should allow for up to 100GbE over 100 meters of cable. Expected availability is in 2013. It has not been approved as a cable standard, and anyone now selling you Cat. 7 cable is fooling you.

REFERENCES:
http://donutey.com/ethernet.php http://en.wikipedia.org/wiki/TIA/EIA-568-B http://en.wikipedia.org/wiki/Category_1_cable

QUESTION 465
Which of the following mechanisms was created to overcome the problem of collisions that occur on wired networks when traffic is simultaneously transmitted from different nodes?

A. Carrier sense multiple access with collision avoidance (CSMA/CA)
B. Carrier sense multiple access with collision detection (CSMA/CD)
C. Polling
D. Token-passing

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:

QUESTION 466
Which of the following does NOT use token-passing?

A. ARCnet
B. FDDI
C. Token-ring
D. IEEE 802.3

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
IEEE 802.3 specifies the standard for Ethernet and uses CSMA/CD, not token-passing.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).

QUESTION 467
What is defined as the manner in which the network devices are organized to facilitate communications?

A. LAN transmission methods
B. LAN topologies
C. LAN transmission protocols
D. LAN media access methods

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A network topology defines the manner in which the network devices are organized to facilitate communications. Common LAN technologies are:

bus
ring
star
meshed

LAN transmission methods refer to the way packets are sent on the network and are:

unicast
multicast
broadcast

LAN transmission protocols are the rules for communicating between computers on a LAN. Common LAN transmission protocols are:

CSMA/CD
polling token-passing

LAN media access methods control the use of a network (physical and data link layers). They can be:

Ethernet
ARCnet
Token ring

FDDI

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 105).

QUESTION 468
Which of the following is a device that is used to regenerate or replicate the received signals?

A. Bridge
B. Router
C. Repeater
D. Brouter

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Repeaters offer the simplest form of connectivity. They regenerate received electrical signals at their original strength between cable segments. Bridges are devices used to connect similar or dissimilar LANs together to form an extended LAN. Routers provide packet routing between network segments. Brouter are devices that combine router and bridge functionality.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

QUESTION 469
Which of the following networking devices allows the connection of two or more homogeneous LANs in a simple way where they forward the traffic based on the MAC address ?

A. Gateways
B. Routers
C. Bridges
D. Firewalls

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Bridges are simple, protocol-dependent networking devices that are used to connect two or more homogeneous LANs to form an extended LAN.

A bridge does not change the contents of the frame being transmitted but acts as a relay.

A gateway is designed to reduce the problems of interfacing any combination of local networks that employ different level protocols or local and long-haul networks.

A router connects two networks or network segments and may use IP to route messages.

Firewalls are methods of protecting a network against security threats from other systems or networks by centralizing and controlling access to the protected network segment.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 397).

QUESTION 470
Which of the following statements pertaining to Asynchronous Transfer Mode (ATM) is false?

A. It can be used for voice
B. it can be used for data
C. It carries various sizes of packets
D. It can be used for video

Correct Answer: C

Section: Network and Telecommunications
Explanation

Explanation/Reference:
ATM is an example of a fast packet-switching network that can be used for either data, voice or video, but packets are of fixed size.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 7: Telecommunications and Network Security (page 455).

QUESTION 471
Which of the following can prevent hijacking of a web session?

A. RSA
B. SET
C. SSL
D. PPP

Correct Answer: C
Section: Network and Telecommunications
Explanation
Explanation/Reference:
The Secure Socket Layer (SSL) protocol is used between a web server and client and provides entire session encryption, thus preventing from session hijacking. RSA is asymmetric encryption algorithm that can be used in setting up a SSL session. SET is the Secure Electronic Transaction protocol that was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. PPP is a point-to-point protocol.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 89).

QUESTION 472
Which type of attack involves impersonating a user or a system?

A. Smurfing attack
B. Spoofing attack
C. Spamming attack
D. Sniffing attack

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
A spoofing attack is when an attempt is made to gain access to a computer system by posing as an authorized user or system. Spamming refers to sending out or posting junk advertising and unsolicited mail. A smurf attack is a type of denial-of-service attack using PING and a spoofed address. Sniffing refers to observing packets passing on a network.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 473
How would an IP spoofing attack be best classified?

A. Session hijacking attack
B. Passive attack
C. Fragmentation attack
D. Sniffing attack

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
IP spoofing is used to convince a system that it is communicating with a known entity that gives an intruder access. IP spoofing attacks is a common session hijacking attack.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 77).

QUESTION 474
What is defined as the rules for communicating between computers on a Local Area Network (LAN)?

A. LAN Media Access methods
B. LAN topologies
C. LAN transmission methods
D. Contention Access Control

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of method must be used to allow one device access to the network media at a time.

This is done in two main ways: carrier sense multiple access collision detect (CSMA/CD) and token passing.

In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred. A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision will not occur again between the two devices. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.

In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic. In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

The following are incorrect answers:
LAN topologies: Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there. Common topologies are: bus, ring, star or meshed. See THIS LINK for more information.

LAN transmission methods: refer to the way packets are sent on the network and are either unicast, multicast or broadcast. See THIS LINK for more information.

Contention Access Control: This is a bogus detractor.
Contention is a real term but Contention Access Control is just made up. Contention methods is very closely related to Media Access Control methods. In communication networks, contention is a media access method that is used to share a broadcast medium. In contention, any computer in the network can transmit data at any time (first come-first served). This system breaks down when two computers attempt to transmit at the same time. This is a case of collision. To avoid collision, carrier sensing mechanism is used. Here each computer listens to the network before attempting to transmit. If the network is busy, it waits until network quiets down. In carrier detection, computers continue to listen to the network as they transmit. If computer detects another signal that interferes with the signal it is sending, it stops transmitting. Both computers then wait for random amount of time and attempt to transmit. Contention methods are most popular media access control method on LANs.

Reference(s) used for this question:
http://docwiki.cisco.com/wiki/Introduction_to_LAN_Protocols#LAN_Media-Access_Methods
http://en.wikipedia.org/wiki/Contention_%28telecommunications%29

QUESTION 475
Which of the following is a LAN transmission method?

A. Broadcast
B. Carrier-sense multiple access with collision detection (CSMA/CD)
C. Token ring
D. Fiber Distributed Data Interface (FDDI)

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.

CSMA/CD is a common LAN media access method.
Token ring is a LAN Topology.
LAN transmission protocols are the rules for communicating between computers on a LAN.
Common LAN transmission protocols are: polling and token-passing.
A LAN topology defines the manner in which the network devices are organized to facilitate communications.
Common LAN topologies are: bus, ring, star or meshed.

LAN transmission methods refer to the way packets are sent on the network and are either unicast, multicast or broadcast.
LAN media access methods control the use of a network (physical and data link layers). They can be Ethernet, ARCnet, Token ring and FDDI.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 103).

HERE IS A NICE OVERVIEW FROM CISCO:
LAN Transmission Methods

LAN data transmissions fall into three classifications: unicast, multicast, and broadcast.
In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network, and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.
LAN Topologies
LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star, and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star. A bus topology is a linear LAN architecture in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks—including 100BaseT—implement a bus topology

Sources:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 104).
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introlan.htm

QUESTION 476
Which of the following LAN topologies offers the highest availability?

A. Bus topology
B. Tree topology
C. Full mesh topology
D. Partial mesh topology

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
In a full mesh topology, all network nodes are individually connected with each other, providing the highest availability. A partial mesh topology can sometimes be used to offer some redundancy.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 106).

QUESTION 477

What is also known as 10Base5?

A. Thinnet
B. Thicknet
C. ARCnet
D. UTP

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Thicknet is a coaxial cable with segments of up to 500 meters, also known as 10Base5. Thinnet is a coaxial cable with segments of up to 185 meters. Unshielded twisted pair (UTP) has three variations: 10 Mbps (10BaseT), 100 Mbps (100BaseT) or 1 Gbps (1000BaseT). ARCnet is a LAN media access method.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 108).

QUESTION 478
Which of the following is an example of a connectionless communication protocol?

A. UDP
B. X.25
C. Packet switching
D. TCP

Correct Answer: A
Section: Network and Telecommunications

Explanation

Explanation/Reference:
UDP is an example of connectionless communication protocol, wherein no connection needs to be established before data can be exchanged.

In telecommunications, connectionless describes communication between two network end points in which a message can be sent from one end point to another without prior arrangement. The device at one end of the communication transmits data addressed to the other, without first ensuring that the recipient is available and ready to receive the data. Some protocols allow for error correction by requested retransmission. Internet Protocol (IP) and User Datagram Protocol (UDP) are connectionless protocols.

Connectionless protocols are also described as stateless because the endpoints have no protocol-defined way to remember where they are in a "conversation" of message exchanges.
List of connectionless protocols

- Hypertext Transfer Protocol
- IP
- UDP
- ICMP
- IPX
- TIPC
- NetBEUI

References:
KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 86).
and
https://secure.wikimedia.org/wikipedia/en/wiki/Connectionless_protocol

QUESTION 479
Which of the following standards is concerned with message handling?

A. X.400
B. X.500
C. X.509
D. X.800

Correct Answer: A

Section: Network and Telecommunications
Explanation

Explanation/Reference:
X.400 is used in e-mail as a message handling protocol. X.500 is used in directory services. X.509 is used in digital certificates and X.800 is used a network security standard.
Reference: http://www.alvestrand.no/x400/.

QUESTION 480
Which of the following IEEE standards defines the token ring media access method?

A. 802.3
B. 802.11
C. 802.5
D. 802.2

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The IEEE 802.5 standard defines the token ring media access method. 802.3 refers to Ethernet's CSMA/CD, 802.11 refers to wireless communications and 802.2 refers to the logical link control.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 109).

QUESTION 481
Which of the following technologies has been developed to support TCP/IP networking over low-speed serial interfaces?

A. ISDN
B. SLIP
C. xDSL
D. T1

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Serial Line IP (SLIP) was developed in 1984 to support TCP/IP networking over low-speed serial interfaces.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 114).

QUESTION 482
What is the main characteristic of a multi-homed host?

A. It is placed between two routers or firewalls.
B. It allows IP routing.
C. It has multiple network interfaces, each connected to separate networks.
D. It operates at multiple layers.

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The main characteristic of a multi-homed host is that is has multiple network interfaces, each connected to logically and physically separate networks. IP routing should be disabled to prevent the firewall from routing packets directly from one interface to the other.

Source: FERREL, Robert G, Questions and Answers for the CISSP Exam, domain 2 (derived from the Information Security Management Handbook, 4th Ed., by Tipton & Krause).

QUESTION 483
What is the main characteristic of a bastion host?

A. It is located on the internal network.
B. It is a hardened computer implementation
C. It is a firewall.
D. It does packet filtering.

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:

A bastion host is a special purpose computer on a network specifically designed and configured to withstand attack. The computer hosts a single application, for example a proxy server, and all other services are removed or limited to reduce the threat to the computer. It is hardened in this manner primarily due to its location and purpose, which is either on the outside of the firewall or in the DMZ and usually involves access from untrusted networks or computers.

References:

http://en.wikipedia.org/wiki/Bastion_host

QUESTION 484
Which of the following statements pertaining to packet switching is incorrect?

A. Most data sent today uses digital signals over network employing packet switching.
B. Messages are divided into packets.
C. All packets from a message travel through the same route.
D. Each network node or point examines each packet for routing.

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
When using packet switching, messages are broken down into packets. Source and destination address are added to each packet so that when passing through a network node, they can be examined and eventually rerouted through different paths as conditions change. All message packets may travel different paths and not arrive in the same order as sent. Packets need to be collected and reassembled into the original message at destination.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 485
All hosts on an IP network have a logical ID called a(n):

A. IP address.
B. MAC address.
C. TCP address.
D. Datagram address.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
All hosts on a network have a logical ID that is called an IP address. An IP address is a numeric identifier that is assigned to each machine on an IP network. It designates the location of a device on a network. A MAC address is typically called a hardware address because it is "burned" into the NIC card. TCP address and Datagram address are imposter answers.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 486
Each data packet is assigned the IP address of the sender and the IP address of the:

A. recipient.
B. host.
C. node.
D. network.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Each data packet is assigned the IP address of the sender and the IP address of the recipient. The term network refers to the part of the IP address that identifies each network. The terms host and node refer to the parts of the IP address that identify a specific machine on a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 487
How long are IPv4 addresses?

A. 32 bits long.
B. 64 bits long.
C. 128 bits long.
D. 16 bits long.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:

IPv4 addresses are currently 32 bits long. IPv6 addresses are 128 bits long.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 488
Which of the following is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
ARP is used to find the Media Access Control address (MAC) that matches with a known Internet Protocol (IP) address.

The Address Resolution Protocol (ARP) is a computer networking protocol for determining a network host's link layer or hardware address when only its Internet Layer (IP) or Network Layer address is known

Reverse Address Resolution Protocol (RARP) is used to find the IP address that matches an Ethernet address.

ICMP is a management protocol and messaging service provider for IP (e.g. PING).
UDP runs over IP. It is a best effort protocol that offers no reliability. UDS is used for application such as streaming media, voice over IP, the DNS protocol, as well as the Simple Network Management Protocol (SNMP).

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.
also see:
http://en.wikipedia.org/wiki/Address_resolution_protocol

QUESTION 489
Address Resolution Protocol (ARP) interrogates the network by sending out a?

A. broadcast.
B. multicast.
C. unicast.
D. semicast.

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
ARP interrogates the network by sending out a broadcast seeking a network node that has a specific IP address, and asks it to reply with its hardware address. A broadcast message is sent to everyone whether or not the message was requested. A traditional unicast is a "one-to-one" or "narrowcast" message. A multicast is a "one-to-many" message that is traditionally only sent to those machine that requested the information. Semicast is an imposter answer.
Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 490
When a station communicates on the network for the first time, which of the following protocol would search for and find the Internet Protocol (IP) address that matches with a known Ethernet address?

A. Address Resolution Protocol (ARP).
B. Reverse Address Resolution Protocol (RARP).
C. Internet Control Message protocol (ICMP).
D. User Datagram Protocol (UDP).

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The RARP protocol sends out a packet, which includes its MAC address and a request to be informed of the IP address that should be assigned to that MAC address.

ARP does the opposite by broadcasting a request to find the Ethernet address that matches a known IP address.

ICMP supports packets containing error, control, and informational messages (e.g. PING).
UDP runs over IP and is used primarily for broadcasting messages over a network.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 87.

QUESTION 491
In order to ensure the privacy and integrity of the data, connections between firewalls over public networks should use:

A. Screened subnets
B. Digital certificates

C. An encrypted Virtual Private Network
D. Encryption

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Virtual Private Networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet.

Screened Subnet: A screened subnet is essentially the same as the screened host architecture, but adds an extra strata of security by creating a network which the bastion host resides (often call perimeter network) which is separated from the internal network. A screened subnet will be deployed by adding a perimeter network in order to separate the internal network from the external. This assures that if there is a successful attack on the bastion host, the attacker is restricted to the perimeter network by the screening router that is connected between the internal and perimeter network.

Digital Certificates: Digital Certificates will be used in the intitial steps of establishing a VPN but they would not provide the encryption and integrity by themselves.

Encryption: Even thou this seems like a choice that would include the other choices, encryption by itself does not provide integrity mechanims. So encryption would satisfy only half of the requirements of the question.

Source: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks (page 65).

QUESTION 492
Which of the following protocols does not operate at the data link layer (layer 2)?

A. PPP
B. RARP
C. L2F
D. ICMP

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
ICMP is the only of the mentioned protocols to operate at the network layer (layer 3). Other protocols operate at layer 2.
Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 493
Which of the following protocols operates at the session layer (layer 5)?

A. RPC
B. IGMP
C. LPD
D. SPX

Correct Answer: A
Section: Network and Telecommunications
Explanation
Explanation/Reference:
Remotre Procedure Call (RPC) is the only of the above choices to operate at the session layer (layer 5).

All of the other answers were wrong.

LPD operates at layer 7
SPX operates at layer 4
IGMP operates at layer 3.

Reference:
WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 494
Which layer of the TCP/IP protocol stack corresponds to the ISO/OSI Network layer (layer 3)?

A. Host-to-host layer
B. Internet layer
C. Network access layer
D. Session layer

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:

The Internet layer in the TCP/IP protocol stack corresponds to the network layer (layer 3) in the OSI/ISO model. The host-to-host layer corresponds to the transport layer (layer 4) in the OSI/ISO model. The Network access layer corresponds to the data link and physical layers (layers 2 and 1) in the OSI/ISO model. The session layer is not defined in the TCP/IP protocol stack.

Source: WALLHOFF, John, CBK#2 Telecommunications and Network Security (CISSP Study Guide), April 2002 (page 1).

QUESTION 495
The concept of best effort delivery is best associated with?

A. TCP
B. HTTP
C. RSVP
D. IP

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The Internet Protocol (IP) is a data-oriented protocol used for communicating data across a packet-switched internetwork. IP provides an unreliable service (i.e., best effort delivery). This means that the network makes no guarantees about the packet.

Low-level connectionless protocols such as DDP (under Appletalk) and IP usually provide best-effort delivery of data.

Best-effort delivery means that the protocol attempts to deliver any packets that meet certain requirements, such as containing a valid destination address, but the protocol does not inform the sender when it is unable to deliver the data, nor does it attempt to recover from error conditions and data loss.

Higher-level protocols such as TCP on the other hand, can provide reliable delivery of data. Reliable delivery includes error checking and recovery from error or loss of data.

HTTP is the HyperText Transport Protocol used to establish connections to a web server and thus one of the higher level protocol using TCP to ensure delivery of all bytes between the client and the server. It was not a good choice according to the question presented.

Here is another definition from the TCP/IP guide at: http://www.tcpipguide.com/free/t_IPOverviewandKeyOperationalCharacteristics.htm

Delivered Unreliably: IP is said to be an “unreliable protocol”. That doesn't mean that one day your IP software will decide to go fishing rather than run your network. J It does mean that when datagrams are sent from device A to device B, device A just sends each one and then moves on to the next. IP doesn't keep track of the ones it sent. It does not provide reliability or service quality capabilities such as error protection for the data it sends (though it does on the IP header), flow control or retransmission of lost datagrams.

For this reason, IP is sometimes called a best-effort protocol. It does what it can to get data to where it needs to go, but “makes no guarantees” that the data will actually get there.

QUESTION 496
Which layer of the OSI/ISO model handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control?

A. Physical
B. Data link

C. Network
D. Session

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The Data Link layer provides data transport across a physical link. It handles physical addressing, network topology, line discipline, error notification, orderly delivery of frames, and optional flow control.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 497
The Logical Link Control sub-layer is a part of which of the following?

A. The ISO/OSI Data Link layer
B. The Reference monitor

C. The Transport layer of the TCP/IP stack model
D. Change management control

Correct Answer: A
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The OSI/ISO Data Link layer is made up of two sub-layers; (1) the Media Access Control layer refers downward to lower layer hardware functions and (2) the Logical Link Control refers upward to higher layer software functions. Other choices are distracters.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 498
Which of the following services relies on UDP?

A. FTP
B. Telnet
C. DNS
D. SMTP

Correct Answer: C
Section: Network and Telecommunications
Explanation

Explanation/Reference:
DNS relies on connectionless UDP whereas services like FTP, Telnet and SMTP rely on TCP.

Source: ROTHKE, Ben, CISSP CBK Review presentation on domain 2, August 1999.

QUESTION 499
How many bits of a MAC address uniquely identify a vendor, as provided by the IEEE?

A. 6 bits
B. 12 bitsC. 16 bits
D. 24 bits

Correct Answer: D
Section: Network and Telecommunications
Explanation

Explanation/Reference:
The MAC address is 48 bits long, 24 of which identify the vendor, as provided by the IEEE. The other 24 bits are provided by the vendor.

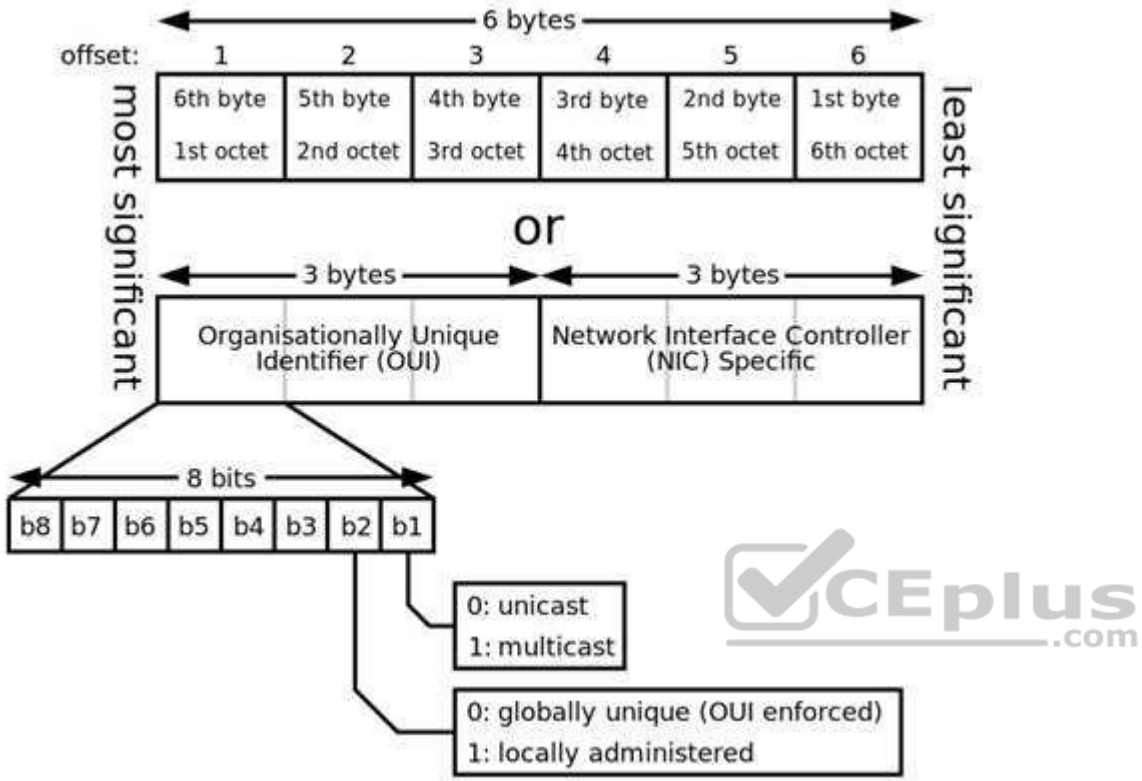
A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface card (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address. It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This is can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address. An example is many SOHO routers, where the ISP grants access to only one MAC address (used previously to inserting the router) so the router must use that MAC address on its Internet-facing NIC. Therefore the router administrator configures a MAC address to override the burned-in one.

A network node may have multiple NICs and each must have one unique MAC address per NIC.

See diagram below from Wikipedia showing the format of a MAC address. :

MAC Address format



Reference(s) used for this question:
http://en.wikipedia.org/wiki/MAC_address

QUESTION 500
Which Network Address Translation (NAT) is the most convenient and secure solution?

A. Hiding Network Address Translation
B. Port Address Translation
C. Dedicated Address Translation
D. Static Address Translation

Correct Answer: B
Section: Network and Telecommunications
Explanation

Explanation/Reference:
Static network address translation offers the most flexibility, but it is not normally practical given the shortage of IP version 4 addresses. Hiding network address translation is was an interim step in the development of network address translation technology, and is seldom used because port address translation offers additional features above and beyond those present in hiding network address translation while maintaining the same basic design and engineering considerations. PAT is often the most convenient and secure solution.

Source: WACK, John et al., NIST Special publication 800-41, Guidelines on Firewalls and Firewall Policy, January 2002 (page 18).