security of computer-based information systems.
The Training Team. Is incorrect because the ultimate responsibility is with management for the security of computer-based information systems.

Reference(s) used for this question:
OIG CBK Information Security Management and Risk Management (page 20 - 22)

QUESTION 339
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
Explanation:
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 340
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
Explanation:
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
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 341
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
Explanation:
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 342
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
Explanation:
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.
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 343
Which of the following embodies all the detailed actions that personnel are required to follow?

A. Standards
B. Guidelines
C. Procedures
D. Baselines

Correct Answer: C
Explanation:
Procedures are step-by-step instructions in support of of the policies, standards, guidelines and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks."

Standards is incorrect. Standards are a "Mandatory statement of minimum requirements that support some part of a policy, the standards in this case is your own company standards and not standards such as the ISO standards"

Guidelines is incorrect. "Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions."

Baselines is incorrect. Baselines "are a minimum acceptable level of security. This minimum is implemented using specific rules necessary to implement the security controls in support of the policy and standards." For example, requiring a password of at leat 8 character would be an example. Requiring all users to have a minimun of an antivirus, a personal firewall, and an anti spyware tool could be another example.

References:
CBK, pp. 12 - 16. Note especially the discussion of the "hammer policy" on pp. 16-17 for the differences between policy, standard, guideline and procedure.
AIO3, pp. 88-93.

QUESTION 344
Making sure that the data has not been changed unintentionally, due to an accident or malice is:

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

Correct Answer: A
Explanation:
Integrity refers to the protection of information from unauthorized modification or deletion.

Confidentiality is incorrect. Confidentiality refers to the protection of information from unauthorized disclosure.

Availability is incorrect. Availability refers to the assurance that information and services will be

available to authorized users in accordance with the service level objective.

Auditability is incorrect. Auditability refers to the ability to trace an action to the identity that performed it and identify the date and time at which it occurred.

References:
CBK, pp. 5 - 6
AIO3, pp. 56 - 57

QUESTION 345
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
Explanation:
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 346
Which of the following are required for Life-Cycle Assurance?

A. System Architecture and Design specification.
B. Security Testing and Covert Channel Analysis.
C. Security Testing and Trusted distribution.
D. Configuration Management and Trusted Facility Management.

Correct Answer: C
Explanation:
Security testing and trusted distribution are required for Life-Cycle Assurance.

The following answers are incorrect:

System Architecture and Design specification. Is incorrect because System Architecture is not requried for Life-Cycle Assurance.
Security Testing and Covert Channel Analysis. Is incorrect because Covert Channel Analysis is not requried for Life-Cycle Assurance.
Configuration Management and Trusted Facility Management. Is incorrect because Trusted Facility Management. is not requried for Life-Cycle Assurance.
QUESTION 347
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
Explanation:
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 348
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
Explanation:
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.