QUESTION 443
A periodic review of user account management should not determine:

A. Conformity with the concept of least privilege.
B. Whether active accounts are still being used.
C. Strength of user-chosen passwords.
D. Whether management authorizations are up-to-date.

Correct Answer: C
Explanation:
Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis.

The strength of user passwords is beyond the scope of a simple user account management review, since it requires specific tools to try and crack the password file/database through either a dictionary or brute-force attack in order to check the strength of passwords.

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 28).

QUESTION 444
Who is responsible for providing reports to the senior management on the effectiveness of the security controls?

A. Information systems security professionals
B. Data owners
C. Data custodians
D. Information systems auditors

Correct Answer: D
Explanation:
IT auditors determine whether systems are in compliance with the security policies, procedures, standards, baselines, designs, architectures, management direction and other requirements" and "provide top company management with an independent view of the controls that have been designed and their effectiveness."

"Information systems security professionals" is incorrect. Security professionals develop the security policies and supporting baselines, etc.

"Data owners" is incorrect. Data owners have overall responsibility for information assets and assign the appropriate classification for the asset as well as ensure that the asset is protected with the proper controls.

"Data custodians" is incorrect. Data custodians care for an information asset on behalf of the data owner.

References:
CBK, pp. 38 - 42.
AIO3. pp. 99 - 104

QUESTION 445
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
Explanation:
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 446
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
Explanation:
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 447
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 system
D. Hackers can circumvent signature evaluations.

Correct Answer: A
Explanation:
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 448
Which of the following questions are least likely to help in assessing controls covering audit trails?

A. Does the audit trail provide a trace of user actions?
B. Are incidents monitored and tracked until resolved?
C. Is access to online logs strictly controlled?
D. Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?

Correct Answer: B
Explanation:
Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide individual accountability, a means to reconstruct events, detect intrusions, and identify problems. Audit trail controls are considered technical controls. Monitoring and tracking of incidents is more an operational control related to incident response capability.

Reference(s) used for this question:

SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-50 to A-51).

NOTE:
NIST SP 800-26 has been superceded By: FIPS 200, SP 800-53, SP 800-53A You can find the new replacement at: http://csrc.nist.gov/publications/PubsSPs.html However, if you really wish to

see the old standard, it is listed as an archived document at:
http://csrc.nist.gov/publications/PubsSPArch.html

QUESTION 449
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
Explanation:
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 450
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
Explanation:
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 451
If an organization were to monitor their employees' e-mail, it should not:

A. Monitor only a limited number of employees.
B. Inform all employees that e-mail is being monitored.
C. Explain who can read the e-mail and how long it is backed up.
D. Explain what is considered an acceptable use of the e-mail system.

Correct Answer: A
Explanation:
Monitoring has to be conducted is a lawful manner and applied in a consistent fashion; thus should be applied uniformly to all employees, not only to a small number.
Source: 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 304).