Regular audit exercise can spot any gap in the information security compliance. Service level monitoring can only pinpoint operational issues in the organization's operational environment. Penetration testing can identify security vulnerability but cannot ensure information compliance Training can increase users' awareness on the information security policy, but is not more effective than auditing.

QUESTION 297
An operating system (OS) noncritical patch to enhance system security cannot be applied because a critical application is not compatible with the change. Which of the following is the BEST solution?

A. Rewrite the application to conform to the upgraded operating system
B. Compensate for not installing the patch with mitigating controls
C. Alter the patch to allow the application to run in a privileged state
D. Run the application on a test platform; tune production to allow patch and application

Correct Answer: B
Explanation:
Since the operating system (OS) patch will adversely impact a critical application, a mitigating control should be identified that will provide an equivalent level of security . Since the application is critical, the patch should not be applied without regard for the application; business requirements must be considered. Altering the OS patch to allow the application to run in a privileged state may create new security weaknesses. Finally, running a production application on a test platform is not an acceptable alternative since it will mean running a critical production application on a platform not subject to the same level of security controls.

QUESTION 298
What is the BEST policy for securing data on mobile universal serial bus (USB) drives?

A. Authentication
B. Encryption
C. Prohibit employees from copying data to I)SB devices
D. Limit the use of USB devices

Correct Answer: B
Explanation:
Encryption provides the most effective protection of data on mobile devices. Authentication on its own is not very secure. Prohibiting employees from copying data to USB devices and limiting the use of USB devices are after the fact.

QUESTION 299
Security monitoring mechanisms should PRIMARILY:

A. focus on business-critical information.
B. assist owners to manage control risks.
C. focus on detecting network intrusions.
D. record all security violations.

Correct Answer: A
Explanation:
Security monitoring must focus on business-critical information to remain effectively usable by

and credible to business users. Control risk is the possibility that controls would not detect an incident or error condition, and therefore is not a correct answer because monitoring would not directly assist in managing this risk. Network intrusions are not the only focus of monitoring mechanisms; although they should record all security violations, this is not the primary objective.

QUESTION 300
Which of the following mechanisms is the MOST secure way to implement a secure wireless network?

A. Filter media access control (MAC) addresses
B. Use a Wi-Fi Protected Access (WPA2) protocol
C. Use a Wired Equivalent Privacy (WEP) key
D. Web-based authentication

Correct Answer: B
Explanation:
WPA2 is currently one of the most secure authentication and encryption protocols for mainstream wireless products. MAC address filtering by itself is not a good security mechanism since allowed MAC addresses can be easily sniffed and then spoofed to get into the network. WEP is no longer a secure encryption mechanism for wireless communications. The WEP key can be easily broken within minutes using widely available software. And once the WEP key is obtained, all communications of every other wireless client are exposed. Finally, a web-based authentication mechanism can be used to prevent unauthorized user access to a network, but it will not solve the wireless network's main security issues, such as preventing network sniffing.

QUESTION 301
Which of the following is the MOST important consideration when implementing an intrusion detection system (IDS)?

A. Tuning
B. Patching
C. Encryption
D. Packet filtering

Correct Answer: A
Explanation:
If an intrusion detection system (IDS) is not properly tuned it will generate an unacceptable number of false positives and/or fail to sound an alarm when an actual attack is underway. Patching is more related to operating system hardening, while encryption and packet filtering would not be as relevant.

QUESTION 302
Which of the following controls would BEST prevent accidental system shutdown from the console or operations area?

A. Redundant power supplies
B. Protective switch covers
C. Shutdown alarms
D. Biometric readers

Correct Answer: B

Explanation:
Protective switch covers would reduce the possibility of an individual accidentally pressing the power button on a device, thereby turning off the device. Redundant power supplies would not prevent an individual from powering down a device. Shutdown alarms would be after the fact. Biometric readers would be used to control access to the systems.

QUESTION 303
A border router should be placed on which of the following?

A. Web server
B. IDS server
C. Screened subnet
D. Domain boundary

Correct Answer: D
Explanation:
A border router should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ) would not provide any protection. Border routers are positioned on the boundary of the network, but do not reside on a server.

QUESTION 304
Which of the following is MOST effective in preventing security weaknesses in operating systems?

A. Patch management
B. Change management
C. Security baselines
D. Configuration management

Correct Answer: A
Explanation:
Patch management corrects discovered weaknesses by applying a correction (a patch) to the original program code. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Configuration management controls the updates to the production environment.

QUESTION 305
On which of the following should a firewall be placed?

A. Web server
B. Intrusion detection system (IDS) server
C. Screened subnet
D. Domain boundary

Correct Answer: D
Explanation:
A firewall should be placed on a (security) domain boundary. Placing it on a web server or screened subnet, which is a demilitarized zone (DMZ), does not provide any protection. Since firewalls should be installed on hardened servers with minimal services enabled, it is inappropriate to have the firewall and the intrusion detection system (IDS) on the same physical device.

QUESTION 306
Which of the following is the MOST important guideline when using software to scan for security exposures within a corporate network?

A. Never use open source tools
B. Focus only on production servers
C. Follow a linear process for attacks
D. Do not interrupt production processes

Correct Answer: D
Explanation:
The first rule of scanning for security exposures is to not break anything. This includes the interruption of any running processes. Open source tools are an excellent resource for performing scans. Scans should focus on both the test and production environments since, if compromised, the test environment could be used as a platform from which to attack production servers. Finally, the process of scanning for exposures is more of a spiral process than a linear process.

QUESTION 307
Which of the following guarantees that data in a file have not changed?

A. Inspecting the modified date of the file
B. Encrypting the file with symmetric encryption
C. Using stringent access control to prevent unauthorized access
D. Creating a hash of the file, then comparing the file hashes

Correct Answer: D
Explanation:
A hashing algorithm can be used to mathematically ensure that data haven't been changed by hashing a file and comparing the hashes after a suspected change.

QUESTION 308
Which of the following would BEST protect an organization's confidential data stored on a laptop computer from unauthorized access?

A. Strong authentication by password
B. Encrypted hard drives
C. Multifactor authentication procedures
D. Network-based data backup

Correct Answer: B
Explanation:
Encryption of the hard disks will prevent unauthorized access to the laptop even when the laptop is lost or stolen. Strong authentication by password can be bypassed by a determined hacker. Multifactor authentication can be bypassed by removal of the hard drive and insertion into another laptop. Network- based data backups do not prevent access but rather recovery from data loss.

QUESTION 309
Which of the following is the BEST method to provide a new user with their initial password for e-mail system access?

A. Interoffice a system-generated complex password with 30 days expiration
B. Give a dummy password over the telephone set for immediate expiration

C. Require no password but force the user to set their own in 10 days
D. Set initial password equal to the user ID with expiration in 30 days

Correct Answer: B
Explanation:
Documenting the password on paper is not the best method even if sent through interoffice mail if the password is complex and difficult to memorize, the user will likely keep the printed password and this creates a security concern. A dummy (temporary) password that will need to be changed upon first logon is the best method because it is reset immediately and replaced with the user's choice of password, which will make it easier for the user to remember. If it is given to the wrong person, the legitimate user will likely notify security if still unable to access the system, so the security risk is low. Setting an account with no initial password is a security concern even if it is just for a few days. Choice D provides the greatest security threat because user IDs are typically known by both users and security staff, thus compromising access for up to 30 days.

QUESTION 310
Which of the following is the MOST important reason for an information security review of contracts? To help ensure that:

A. the parties to the agreement can perform.
B. confidential data are not included in the agreement.
C. appropriate controls are included.
D. the right to audit is a requirement.

Correct Answer: C
Explanation:
Agreements with external parties can expose an organization to information security risks that must be assessed and appropriately mitigated. The ability of the parties to perform is normally the responsibility of legal and the business operation involved. Confidential information may be in the agreement by necessity and. while the information security manager can advise and provide approaches to protect the information, the responsibility rests with the business and legal. Audit rights may be one of many possible controls to include in a third-party agreement, but is not necessarily a contract requirement, depending on the nature of the agreement.

QUESTION 311
An outsource service provider must handle sensitive customer information. Which of the following is MOST important for an information security manager to know?

A. Security in storage and transmission of sensitive data
B. Provider's level of compliance with industry standards
C. Security technologies in place at the facility
D. Results of the latest independent security review

Correct Answer: A
Explanation:
Mow the outsourcer protects the storage and transmission of sensitive information will allow an information security manager to understand how sensitive data will be protected. Choice B is an important but secondary consideration. Choice C is incorrect because security technologies are not the only components to protect the sensitive customer information. Choice D is incorrect because an independent security review may not include analysis on how sensitive customer information would be protected.