QUESTION 350
Which of the following is held accountable for the risk to organizational systems and data that result from outsourcing Information Technology (IT) systems and services?

A. The acquiring organization
B. The service provider
C. The risk executive (function)
D. The IT manager

Answer: C

QUESTION 351
Which of the following is the BEST definition of Cross-Site Request Forgery (CSRF)?

A. An attack which forces an end user to execute unwanted actions on a web application in which they are currently authenticated
B. An attack that injects a script into a web page to execute a privileged command
C. An attack that makes an illegal request across security zones and thereby forges itself into the security database of the system
D. An attack that forges a false Structure Query Language (SQL) command across systems

Answer: A

QUESTION 352
Which of the following is a process in the access provisioning lifecycle that will MOST likely identify access aggregation issues?

A. Test
B. Assessment
C. Review
D. Peer review

Answer: C

QUESTION 353
Which of the following is the PRIMARY reason a sniffer operating on a network is collecting packets only from its own host?

A. An Intrusion Detection System (IDS) has dropped the packets.
B. The network is connected using switches.

C. The network is connected using hubs.
D. The network's firewall does not allow sniffing.

Answer: A

QUESTION 354
Which of the following is the final phase of the identity and access provisioning lifecycle?

A. Recertification
B. Revocation
C. Removal
D. Validation

Answer: B

QUESTION 355
Which of the following is mobile device remote fingerprinting?

A. Installing an application to retrieve common characteristics of the device
B. Storing information about a remote device in a cookie file
C. Identifying a device based on common characteristics shared by all devices of a certain type
D. Retrieving the serial number of the mobile device

Answer: C

QUESTION 356
Which of the following trust services principles refers to the accessibility of information used by the systems, products, or services offered to a third-party provider's customers?

A. Security
B. Privacy
C. Access
D. Availability

Answer: C

QUESTION 357
Which of the following open source software issues pose the MOST risk to an application?

A. The software is beyond end of life and the vendor is out of business.
B. The software is not used or popular in the development community.
C. The software has multiple Common Vulnerabilities and Exposures (CVE) and only some are remediated.
D. The software has multiple Common Vulnerabilities and Exposures (CVE) but the CVEs are classified as low risks.

Answer: D

QUESTION 358
Which of the following is the PRIMARY mechanism used to limit the range of objects available to a given subject within different execution domains?

A. Process isolation
B. Data hiding and abstraction
C. Use of discrete layering and Application Programming Interfaces (API)

D. Virtual Private Network (VPN)

Answer: C

QUESTION 359
Once the types of information have been identified, who should an information security practitioner work with to ensure that the information is properly categorized?

A. Information Owner (IO)
B. System Administrator
C. Business Continuity (BC) Manager
D. Chief Information Officer (CIO)

Answer: A

QUESTION 360
What should be the FIRST action for a security administrator who detects an intrusion on the network based on precursors and other indicators?

A. Isolate and contain the intrusion.
B. Notify system and application owners.
C. Apply patches to the Operating Systems (OS).
D. Document and verify the intrusion.

Answer: C

QUESTION 361
Which of the following needs to be taken into account when assessing vulnerability?

A. Risk identification and validation
B. Threat mapping
C. Risk acceptance criteria
D. Safeguard selection

Answer: A