Management may develop a contingency plan if the risk does occur. Acceptance response to a risk event is a strategy that can be used for risks that pose either threats or opportunities.

Acceptance response can be of two types: Passive acceptance: It is a strategy in which no plans are made to try or avoid or mitigate the risk. Active acceptance: Such responses include developing contingency reserves to deal with risks, in case they occur. Acceptance is the only response for both threats and opportunities. Answer: B is incorrect. Mitigation aims to lower the probability and/or impact of the risk event. Answer: C is incorrect. Transference transfers the ownership of the risk event to a third party, usually through a contractual agreement. Answer: D is incorrect. Enhance is a risk response that tries to increase the probability and/or impact of the positive risk event.

QUESTION 205

Mark is the project manager of the NHQ project in StarTech Inc. The project has an asset valued at $195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

A. $68,250
B. $92,600
C. $72,650
D. $67,250

Answer: A

Explanation:

The Single Loss Expectancy (SLE) of this project will be $68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows: Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed. Here, it is as follows:

SLE = Asset Value * Exposure Factor

= 195,000 * 0.35

= $68,250

Answer: B, C, and D are incorrect. These are not valid SLE's for this project.

QUESTION 206

FIPS 199 defines the three levels of potential impact on organizations: low, moderate, and high. Which of the following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact?

A. The loss of confidentiality, integrity, or availability might result in a major damage to organizational assets.
B. The loss of confidentiality, integrity, or availability might result in severe damages like life threatening injuries or loss of life.
C. The loss of confidentiality, integrity, or availability might result in major financial losses.
D. The loss of confidentiality, integrity, or availability might cause severe degradation in or loss of mission capability to an extent.

Answer: ABCD

Explanation:
The following are the effects of loss of confidentiality, integrity, or availability in a high level potential impact: It might cause a severe degradation in or loss of mission capability to an extent. It might result in a major damage to organizational assets. It might result in a major financial loss. It might result in severe harms such as serious life threatening injuries or loss of life.

QUESTION 207
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

A. SNMP enumeration
B. IIS buffer overflow
C. NetBIOS NULL session
D. DNS zone transfer

Answer: B
Explanation:
Removing the IPP printing capability from a server is a good countermeasure against an IIS buffer overflow attack. A Network Administrator should take the following steps to prevent a Web server from IIS buffer overflow attacks: Conduct frequent scans for server vulnerabilities. Install the upgrades of Microsoft service packs.

Implement effective firewalls. Apply URLScan and IISLockdown utilities. Remove the IPP printing capability. Answer: D is incorrect. The following are the DNS zone transfer countermeasures: Do not allow DNS zone transfer using the DNS property sheet: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the Zone Transfer tab, clear the Allow zone transfers check box. Configure the master DNS server to allow zone transfers only from secondary DNS servers: a.Open DNS. b.Right-click a DNS zone and click Properties. c.On the zone transfer tab, select the Allow zone transfers check box, and then do one of the following: To allow zone transfers only to the DNS servers listed on the name servers tab, click on the Only to the servers listed on the Name Server tab. To allow zone transfers only to specific DNS servers, click Only to the following servers, and add the IP address of one or more servers. Deny all unauthorized inbound connections to TCP port 53. Implement DNS keys and encrypted DNS payloads. Answer: A is incorrect. The following are the countermeasures against SNMP enumeration: 1.Removing the SNMP agent or disabling the SNMP service 2.Changing the default PUBLIC community name when 'shutting off SNMP' is not an option 3.Implementing the Group Policy security option called Additional restrictions for anonymous connections 4.Restricting access to NULL session pipes and NULL session shares 5.Upgrading SNMP Version 1 with the latest version 6.Implementing Access control list filtering to allow only access to the read-write community from approved stations or subnets Answer: C is incorrect. NetBIOS NULL session vulnerabilities are hard to prevent, especially if NetBIOS is needed as part of the infrastructure. One or more of the following steps can be taken to limit NetBIOS NULL session vulnerabilities: 1.Null sessions require access to the TCP 139 or TCP 445 port, which can be disabled by a Network Administrator. 2.A Network Administrator can also disable SMB services entirely on individual hosts by unbinding WINS Client TCP/IP from the interface. 3.A Network Administrator can also restrict the anonymous user by editing the registry values: a.Open regedit32, and go to HKLM\SYSTEM\CurrentControlSet\LSA. b.Choose edit > add value. Value name:

RestrictAnonymous Data Type: REG_WORD Value: 2

QUESTION 208
Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Open-box
B. Closed-box
C. Zero-knowledge test
D. Full-box
E. Full-knowledge test
F. Partial-knowledge test

Answer: ABCEF
Explanation:
The different categories of penetration testing are as follows: Open-box: In this category of penetration testing, testers have access to internal system code. This mode is basically suited for Unix or Linux. Closed-box: In this category of penetration testing, testers do not have access to closed systems. This method is good for closed systems. Zero-knowledge test: In this category of penetration testing, testers have to acquire information from scratch and they are not supplied with information concerning the IT system. Partial-knowledge test: In this category of penetration testing, testers have knowledge that may be applicable to a specific type of attack and associated vulnerabilities. Full-knowledge test: In this category of penetration testing, testers have massive knowledge concerning the information system to be evaluated. Answer: D is incorrect. There is no such category of penetration testing.

QUESTION 209
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: C
Explanation:
Confidentiality is violated in a shoulder surfing attack. The CIA triad provides the following three tenets for which security practices are measured: Confidentiality: It is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Integrity: It means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. Availability: It means that data must be available at every time when it is needed. Answer: D is incorrect. Authenticity is not a tenet of the CIA triad.

QUESTION 210
Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

A. Act honorably, honestly, justly, responsibly, and legally.
B. Give guidance for resolving good versus good and bad versus bad dilemmas.
C. Provide diligent and competent service to principals.
D. Protect society, the commonwealth, and the infrastructure.

Answer: ACD
Explanation:
The Code of Ethics Canons in (ISC)2 code of ethics are as follows: Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally. Provide diligent and competent service to principals. Advance and protect the profession.

QUESTION 211
The Systems Development Life Cycle (SDLC) is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. Which of the following are the different phases of system development life cycle? Each correct answer represents a complete solution. Choose all that apply.

A. Testing
B. Implementation
C. Operation/maintenance
D. Development/acquisition
E. Disposal
F. Initiation

Answer: BCDEF
Explanation:
The Systems Development Life Cycle (SDLC), or Software Development Life Cycle in systems engineering, information systems, and software engineering, is the process of creating or altering the systems; and the models and methodologies that people use to develop these systems. The concept generally refers to computers or information systems. The following are the five phases in a generic System Development Life Cycle: 1.Initiation 2.Development/acquisition 3.Implementation 4.Operation/maintenance 5.Disposal

QUESTION 212
The service-oriented modeling framework (SOMF) introduces five major life cycle modeling activities that drive a service evolution during design-time and run-time. Which of the following activities integrates SOA software assets and establishes SOA logical environment dependencies?

A. Service-oriented discovery and analysis modeling
B. Service-oriented business integration modeling
C. Service-oriented logical architecture modeling
D. Service-oriented logical design modeling

Answer: C
Explanation:
The service-oriented logical architecture modeling integrates SOA software assets and establishes SOA logical environment dependencies. It also offers foster service reuse, loose

coupling and consolidation. Answer: A is incorrect. The service-oriented discovery and analysis modeling discovers and analyzes services for granularity, reusability, interoperability, loose-coupling, and identifies consolidation opportunities. Answer: B is incorrect. The service-oriented business integration modeling identifies service integration and alignment opportunities with business domains' processes. Answer: D is incorrect. The service-oriented logical design modeling establishes service relationships and message exchange paths.

QUESTION 213
Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

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

Answer: BCD
Explanation:
The following concepts represent the three fundamental principles of information security: 1.Confidentiality 2.Integrity 3.Availability Answer: B is incorrect. Privacy, authentication, accountability, authorization and identification are also concepts related to information security, but they do not represent the fundamental principles of information security.

QUESTION 214
Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the we-are-secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

A. Smurf dos attack
B. Land attack
C. Ping flood attack
D. Teardrop attack

Answer: C
Explanation:
According to the scenario, Samantha is using the ping flood attack. In a ping flood attack, an attacker sends a large number of ICMP packets to the target computer using the ping command, i.e., ping -f target_IP_address. When the target computer receives these packets in large quantities, it does not respond and hangs. However, for such an attack to take place, the attacker must have sufficient Internet bandwidth, because if the target responds with an "ECHO reply ICMP packet" message, the attacker must have both the incoming and outgoing bandwidths available for communication. Answer: A is incorrect. In a smurf DoS attack, an attacker sends a large amount of ICMP echo request traffic to the IP broadcast addresses. These ICMP requests have a spoofed source address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all the hosts, most of the IP addresses send an ECHO reply message. However, on a multi- access broadcast network, hundreds of computers might reply to each packet when the target network is overwhelmed by all the messages sent simultaneously. Due to this, the network becomes unable to provide services to all the messages and crashes. Answer: D is incorrect. In a teardrop attack, a series of data packets are sent to the target computer with overlapping offset field values. As a result, the target computer is unable to reassemble these packets and is forced to crash, hang, or reboot. Answer: