QUESTION 183
Which of the following security models dictates that subjects can only access objects through applications?

A. Biba model
B. Bell-LaPadula
C. Clark-Wilson
D. Biba-Clark model

Answer: C
Explanation:
The Clark-Wilson security model dictates that subjects can only access objects through applications. Answer: A is incorrect. The Biba model does not let subjects write to objects at a higher integrity level. Answer: B is incorrect. The Bell-LaPadula model has a simple security rule, which means a subject cannot read data from a higher level. Answer: D is incorrect. There is no such model as Biba-Clark model.

QUESTION 184
The Project Risk Management knowledge area focuses on which of the following processes? Each correct answer represents a complete solution. Choose all that apply.

A. Risk Monitoring and Control
B. Risk Management Planning
C. Quantitative Risk Analysis
D. Potential Risk Monitoring

Answer: ABC
Explanation:
The Project Risk Management knowledge area focuses on the following processes: Risk Management Planning Risk Identification Qualitative Risk Analysis Quantitative Risk Analysis Risk Response Planning Risk Monitoring and Control Answer: D is incorrect. There is no such process in the Project Risk Management knowledge area.

QUESTION 185
Which of the following is used by attackers to record everything a person types, including usernames, passwords, and account information?

A. Packet sniffing
B. Keystroke logging
C. Spoofing
D. Wiretapping

Answer: B
Explanation:
Keystroke logging is used by attackers to record everything a person types, including usernames, passwords, and account information. Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or hardware devices. Keystroke logging devices can record everything a person types using his keyboard, such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used to get usernames, passwords, etc. Answer: D is incorrect. Wiretapping is used to eavesdrop on voice calls. Eavesdropping is the process of listening in on private conversations. It also includes attackers

listening in on network traffic. Answer: C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer: A is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet-sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

QUESTION 186
Which of the following policies can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations?

A. Informative
B. Advisory
C. Selective
D. Regulatory

Answer: A
Explanation:
An informative policy informs employees about certain topics. It is not an enforceable policy, but rather one to teach individuals about specific issues relevant to the company. The informative policy can explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations. Answer: D is incorrect. A regulatory policy ensures that an organization follows the standards set by specific industry regulations. This type of policy is very detailed and specific to a type of industry. The regulatory policy is used in financial institutions, health care facilities, public utilities, and other government-regulated industries, e.g., TRAI. Answer: B is incorrect. An advisory policy strongly advises employees regarding which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if employees do not comply with the established behaviors and activities. The advisory policy can be used to describe how to handle medical information, handle financial transactions, and process confidential information. Answer: C is incorrect. It is not a valid type of policy.

QUESTION 187
Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

A. Single Loss Expectancy (SLE)
B. Annualized Rate of Occurrence (ARO)
C. Safeguard
D. Exposure Factor (EF)

Answer: B
Explanation:
The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event

occurring and the number of employees that could make that event occur. Answer: D is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer: A is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event. SLE = Asset Value ($) X Exposure Factor (EF) Answer: C is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

QUESTION 188
What are the subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process? Each correct answer represents a complete solution. Choose all that apply.

A. Conduct validation activities.
B. Execute and update IA implementation plan.
C. Combine validation results in DIACAP scorecard.
D. Conduct activities related to the disposition of the system data and objects.

Answer: ABC
Explanation:
The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. The subordinate tasks of the Implement and Validate Assigned IA Control phase in the DIACAP process are as follows: Execute and update IA implementation plan. Conduct validation activities. Combine validation results in the DIACAP scorecard. Answer: D is incorrect. The activities related to the disposition of the system data and objects are conducted in the fifth phase of the DIACAP process. The fifth phase of the DIACAP process is known as Decommission System.

QUESTION 189
Which of the following is an open source network intrusion detection system?

A. NETSH
B. Macof
C. Sourcefire
D. Snort

Answer: D
Explanation:
Snort is an open source network intrusion prevention and detection system that operates as a network sniffer. It logs activities of the network that is matched with the predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP). The three main modes in which Snort can be configured are as follows:

Sniffer mode: It reads the packets of the network and displays them in a continuous stream on the console. Packet logger mode: It logs the packets to the disk. Network intrusion detection mode: It is the most complex and configurable configuration, allowing Snort to analyze network traffic for matches against a user-defined rule set. Answer: B is incorrect. Macof is a tool of the dsniff tool set and used to flood the local network with random MAC addresses. It causes some switches to fail open in repeating mode, and facilitates sniffing. Answer: C is incorrect. Sourcefire is the company that owns and maintains Snort. Answer: A is incorrect. NETSH is not a network intrusion detection system. NETSH is a command line tool to configure TCP/IP settings such as the IP address, Subnet Mask, Default Gateway, DNS, WINS addresses, etc.

QUESTION 190
You work as a Security Manager for Tech Perfect Inc. The company has a Windows based network. It is required to determine compatibility of the systems with custom applications. Which of the following techniques will you use to accomplish the task?

A. Safe software storage
B. Antivirus management
C. Backup control
D. Software testing

Answer: D
Explanation:
In order to accomplish the task, you should use the software testing technique. By using this technique you can determine compatibility of systems with custom applications or you can identify other unforeseen interactions. You can also use the software testing technique while you are upgrading software. Answer: B is incorrect. You can use the antivirus management to save the systems from viruses, unexpected software interactions, and the subversion of security controls. Answer: A is incorrect. You can use the safe software storage technique to ensure that the software and backup copies have not been modified without authorization. Answer: C is incorrect. You can use the backup control to perform back up of software and data.

QUESTION 191
Adrian is the project manager of the NHP Project. In her project there are several work packages that deal with electrical wiring. Rather than to manage the risk internally she has decided to hire a vendor to complete all work packages that deal with the electrical wiring. By removing the risk internally to a licensed electrician Adrian feels more comfortable with project team being safe. What type of risk response has Adrian used in this example?

A. Acceptance
B. Avoidance
C. Mitigation
D. Transference

Answer: D
Explanation:
This is an example of transference. When the risk is transferred to a third party, usually for a fee, it creates a contractual-relationship for the third party to manage the risk on behalf of the performing organization. Risk response planning is a method of developing options to decrease the amount of threats and make the most of opportunities. The risk response should be aligned with the consequence of the risk and cost-effectiveness. This planning documents the processes for managing risk events. It addresses the owners and their responsibilities, risk identification, results from qualification and quantification processes, budgets and times for responses, and contingency plans. The various risk response planning techniques are as follows: Risk acceptance: It indicates that the project team has decided not to change the project management plan to deal with a risk, or is unable to identify any other suitable response strategy. Risk avoidance: It is a technique for a threat, which creates changes to the project management plan that are meant to either eliminate the risk or to protect the project objectives from this impact. Risk mitigation: It is a list of specific actions being taken to deal with specific risks associated with the threats and seeks to reduce the probability of occurrence or impact of risk below an acceptable threshold. Risk transference: It is used to shift the impact of a threat to a third party, together with the ownership of the response.

QUESTION 192
You work as a CSO (Chief Security Officer) for Tech Perfect Inc. You have a disaster scenario and you want to discuss it with your team members for getting appropriate responses of the disaster. In which of the following disaster recovery tests can this task be performed?

A. Structured walk-through test
B. Full-interruption test
C. Parallel test
D. Simulation test

Answer: D
Explanation:
A simulation test is a method used to test the disaster recovery plans. It operates just like a structured walk-through test. In the simulation test, the members of a disaster recovery team present with a disaster scenario and then, discuss on appropriate responses. These suggested responses are measured and some of them are taken by the team. The range of the simulation test should be defined carefully for avoiding excessive disruption of normal business activities. Answer: A is incorrect. The structured walk-through test is also known as the table-top exercise. In structured walk-through test, the team members walkthrough the plan to identify and correct weaknesses and how they will respond to the emergency scenarios by stepping in the course of the plan. It is the most effective and competent way to identify the areas of overlap in the plan before conducting more challenging training exercises. Answer: B is incorrect. A full-interruption test includes the operations that shut down at the primary site and are shifted to the recovery site according to the disaster recovery plan. It operates just like a parallel test. The full-interruption test is very expensive and difficult to arrange. Sometimes, it causes a major disruption of operations if the test fails. Answer: C is incorrect. A parallel test includes the next level in the testing procedure, and relocates the employees to an alternate recovery site and implements site activation procedures. These employees present with their disaster recovery responsibilities as they would for an actual disaster. The disaster recovery sites have full responsibilities to conduct the day-to- day organization's business.

QUESTION 193
Which of the following is the most secure method of authentication?

A. Biometrics
B. Username and password
C. Anonymous
D. Smart card

Answer: A
Explanation:
Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment. It is the most secure method of authentication. Answer: B is incorrect. Username and password is the least secure method of authentication in comparison of smart card and biometrics authentication. Username and password can be intercepted. Answer: D is incorrect. Smart card authentication is not as reliable as biometrics authentication. Answer: C is incorrect. Anonymous authentication does not provide security as a user can log on to the system anonymously and he is not prompted for credentials.

QUESTION 194