C. Full-interruption test
D. Checklist test

Answer: D
Explanation:
A checklist test is a test in which the disaster recovery checklists are distributed to the members of the disaster recovery team. All members are asked to review the assigned checklist. The checklist test is a simple test and it is easy to conduct this test. It allows to accomplish the following three goals: It ensures that the employees are aware of their responsibilities and they have the refreshed knowledge. It provides an individual with an opportunity to review the checklists for obsolete information and update any items that require modification during the changes in the organization. It ensures that the assigned members of disaster recovery team are still working for the organization. Answer: B is incorrect. 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. 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. Answer: C 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.

QUESTION 22
CORRECT TEXT
Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.

Answer: Life cycle
Explanation:
A life cycle model helps to provide an insight into the development process and emphasizes on the relationships among the different activities in this process. This model describes a structured approach to the development and adjustment process involved in producing and maintaining systems. The life cycle model addresses specifications, design, requirements, verification and validation, and maintenance activities.

QUESTION 23
Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?

A. Secure assertion
B. Authenticated session
C. Password propagation
D. Account lockout

Answer: C
Explanation:
Password propagation provides an alternative by requiring that a user's authentication credentials

be verified by the database before providing access to that user's data. Answer: D is incorrect. Account lockout implements a limit on the incorrect password attempts to protect an account from automated password-guessing attacks. Answer: B is incorrect. Authenticated session allows a user to access more than one access-restricted Web page without re-authenticating every page. It also integrates user authentication into the basic session model. Answer: A is incorrect. Secure assertion distributes application-specific sanity checks throughout the system.

QUESTION 24
Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?

A. RTO
B. RTA
C. RPO
D. RCO

Answer: A
Explanation:
The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users. Decision time for user representative is not included. The business continuity timeline usually runs parallel with an incident management timeline and may start at the same, or different, points. In accepted business continuity planning methodology, the RTO is established during the Business Impact Analysis (BIA) by the owner of a process (usually in conjunction with the Business Continuity planner). The RTOs are then presented to senior management for acceptance. The RTO attaches to the business process and not the resources required to support the process. Answer: B is incorrect. The Recovery Time Actual (RTA) is established during an exercise, actual event, or predetermined based on recovery methodology the technology support team develops. This is the time frame the technology support takes to deliver the recovered infrastructure to the business. Answer: D is incorrect. The Recovery Consistency Objective (RCO) is used in Business Continuity Planning in addition to Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It applies data consistency objectives to Continuous Data Protection services. Answer: C is incorrect. The Recovery Point Objective (RPO) describes the acceptable amount of data loss measured in time. It is the point in time to which data must be recovered as defined by the organization. The RPO is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation. If the RPO of a company is 2 hours and the time it takes to get the data back into production is 5 hours, the RPO is still 2 hours. Based on this RPO the data must be restored to within 2 hours of the disaster.

QUESTION 25
Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?

A. Information Assurance (IA)
B. Information systems security engineering (ISSE)
C. Certification and accreditation (C&A)
D. Risk Management

Answer: C
Explanation:

Certification and accreditation (C&A) is a set of processes that culminate in an agreement between key players that a system in its current configuration and operation provides adequate protection controls. Certification and Accreditation (C&A or CnA) is a process for implementing information security. It is a systematic procedure for evaluating, describing, testing, and authorizing systems prior to or after a system is in operation. The C&A process is used extensively in the U.S. Federal Government. Some C&A processes include FISMA, NIACAP, DIACAP, and DCID 6/3. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. Answer: D is incorrect. Risk management is a set of processes that ensures a risk-based approach is used to determine adequate, cost- effective security for a system. Answer: A is incorrect. Information assurance (IA) is the process of organizing and monitoring information-related risks. It ensures that only the approved users have access to the approved information at the approved time. IA practitioners seek to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability, and non-repudiation. These objectives are applicable whether the information is in storage, processing, or transit, and whether threatened by an attack. Answer B is incorrect. ISSE is a set of processes and solutions used during all phases of a system's life cycle to meet the system's information protection needs.

QUESTION 26
Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

A. Espionage law
B. Trademark law
C. Cyber law
D. Copyright law

Answer: B
Explanation:
The Trademark law is a piece of legislation that contains the federal statutes of trademark law in the United States. The Act prohibits a number of activities, including trademark infringement, trademark dilution, and false advertising. Trademarks were traditionally protected in the United States only under State common law, growing out of the tort of unfair competition. Trademark law in the United States is almost entirely enforced through private lawsuits. The exception is in the case of criminal counterfeiting of goods. Otherwise, the responsibility is entirely on the mark owner to file suit in either state or federal civil court in order to restrict an infringing use. Failure to "police" a mark by stopping infringing uses can result in the loss of protection. Answer: D is incorrect. Copyright law of the United States governs the legally enforceable rights of creative and artistic works under the laws of the United States. Copyright law in the United States is part of federal law, and is authorized by the U.S. Constitution. The power to enact copyright law is granted in Article I, Section 8, Clause 8, also known as the Copyright Clause. This clause forms the basis for U.S. copyright law ("Science", "Authors", "Writings") and patent law ("useful Arts",

"Inventors", "Discoveries"), and includes the limited terms (or durations) allowed for copyrights and patents ("limited Times"), as well as the items they may protect. In the U.S., registrations of claims of copyright, recordation of copyright transfers, and other administrative aspects of copyright are the responsibility of the United States Copyright Office, a part of the Library of Congress. Answer: A is incorrect. The Espionage Act of 1917 was a United States federal law passed shortly after entering World War I, on June 15, 1917, which made it a crime for a person: To convey information with intent to interfere with the operation or success of the armed forces of the United States or to promote the success of its enemies. This was punishable by death or by imprisonment for not more than 30 years. To convey false reports or false statements with intent to interfere with the operation or success of the military or naval forces of the United States or to promote the success of its enemies and whoever when the United States is at war, to cause or attempt to cause insubordination, disloyalty, mutiny, refusal of duty, in the military or naval forces of the United States, or to willfully obstruct the recruiting or enlistment service of the United States. Answer: C is incorrect. Cyber law is a very wide term, which wraps up the legal issue related to the use of communicative, transactional and distributive aspect of networked information device and technologies. It is commonly known as INTERNET LAW. These Laws are important to apply as Internet does not tend to make any geographical and jurisdictional boundaries clear; this is the reason why Cyber law is not very efficient. A single transaction may involve the laws of at least three jurisdictions, which are as follows: 1.The laws of the state/nation in which the user resides 2.The laws of the state/nation that apply where the server hosting the transaction is located 3.The laws of the state/nation, which apply to the person or business with whom the transaction takes place

QUESTION 27
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?

A. Perform OS fingerprinting on the We-are-secure network.
B. Map the network of We-are-secure Inc.
C. Install a backdoor to log in remotely on the We-are-secure server.
D. Fingerprint the services running on the we-are-secure network.

Answer: A
Explanation:
John will perform OS fingerprinting on the We-are-secure network. Fingerprinting is the easiest way to detect the Operating System (OS) of a remote system. OS detection is important because, after knowing the target system's OS, it becomes easier to hack into the system. The comparison of data packets that are sent by the target system is done by fingerprinting. The analysis of data packets gives the attacker a hint as to which operating system is being used by the remote system. There are two types of fingerprinting techniques as follows: 1.Active fingerprinting 2.Passive fingerprinting In active fingerprinting ICMP messages are sent to the target system and the response message of the target system shows which OS is being used by the remote system. In passive fingerprinting the number of hops reveals the OS of the remote system. Answer: D and B are incorrect. John should perform OS fingerprinting first, after which it will be easy to identify which services are running on the network since there are many services that run only on a specific operating system. After performing OS fingerprinting, John should perform networking mapping. Answer: C is incorrect. This is a pre-attack phase, and only after gathering all relevant knowledge of a network should John install a backdoor.

QUESTION 28

Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?

A. Phase 4
B. Phase 3
C. Phase 1
D. Phase 2

Answer: D
Explanation:
The Phase 2 of DITSCAP C&A is known as Verification. The goal of this phase is to obtain a fully integrated system for certification testing and accreditation. This phase takes place between the signing of the initial version of the SSAA and the formal accreditation of the system. This phase verifies security requirements during system development. Answer: C, B, and A are incorrect. These phases do not take place between the signing of the initial version of the SSAA and the formal accreditation of the system.

QUESTION 29
In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?

A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test

Answer: B
Explanation:
A penetration testing is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of an attack and the amount of business impact of a successful exploit, if discovered. It is a component of a full security audit. Answer: C is incorrect. A paper test is the least complex test in the disaster recovery and business continuity testing approaches. In this test, the BCP/DRP plan documents are distributed to the appropriate managers and BCP/DRP team members for review, markup, and comment. This approach helps the auditor to ensure that the plan is complete and that all team members are familiar with their responsibilities within the plan. Answer: D is incorrect. A walk-through test is an extension of the paper testing in the business continuity and disaster recovery process. In this testing methodology, appropriate managers and BCP/DRP team members discuss and walk through procedures of the plan. They also discuss the training needs, and clarification of critical plan elements. Answer: A is incorrect. A full operational test includes all team members and participants in the disaster recovery and business continuity process. This full operation test involves the mobilization of personnel. It restores operations in the same manner as an outage or disaster would. The full operational test extends the preparedness test by including actual notification, mobilization of resources, processing of data, and utilization of backup media for restoration.