**Explanation:**
Data remanence refers to the data that remains even after the efforts have been made for removing or erasing the data. This event occurs because of data being left intact by an insignificant file deletion operation, by storage media reformatting, or through physical properties of the storage medium. Data remanence can make unintentional disclosure of sensitive information possible. So, it is required that the storage media is released into an uncontrolled environment. Answer: C and B are incorrect. These are the made-up disasters. Answer: A is incorrect. Object reuse refers to reassigning some other object of a storage media that has one or more objects.

**QUESTION 52**
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. Which of the following statements are true about Certification and Accreditation? Each correct answer represents a complete solution. Choose two.

A. Certification is a comprehensive assessment of the management, operational, and technical security controls in an information system.
B. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
C. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
D. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

**Answer:** AC
**Explanation:**
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.

**QUESTION 53**
The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. What are the process activities of this phase? Each correct answer represents a complete solution. Choose all that apply.

A. Negotiation
B. Registration
C. Document mission need
D. Initial Certification Analysis

**Answer:** ABC
**Explanation:**
The Phase 1 of DITSCAP C&A is known as Definition Phase. The goal of this phase is to define the C&A level of effort, identify the main C&A roles and responsibilities, and create an agreement on the method for implementing the security requirements. The Phase 1 starts with the input of the mission need. This phase comprises three process activities: Document mission need Registration Negotiation Answer: D is incorrect. Initial Certification Analysis is a Phase 2 activity.

**QUESTION 54**
Which of the following NIST Special Publication documents provides a guideline on network security testing?

A. NIST SP 800-42
B. NIST SP 800-53A
C. NIST SP 800-60
D. NIST SP 800-53
E. NIST SP 800-37
F. NIST SP 800-59

**Answer:** A
**Explanation:**
NIST SP 800-42 provides a guideline on network security testing. Answer: E, D, B, F, and C are incorrect. NIST has developed a suite of documents for conducting Certification & Accreditation (C&A). These documents are as follows: NIST Special Publication 800-37: This document is a guide for the security certification and accreditation of Federal Information Systems. NIST Special Publication 800-53: This document provides a guideline for security controls for Federal Information Systems. NIST Special Publication 800-53A. This document consists of techniques and procedures for verifying the effectiveness of security controls in Federal Information System. NIST Special Publication 800-59: This document is a guideline for identifying an information system as a National Security System. NIST Special Publication 800-60: This document is a guide for mapping types of information and information systems to security objectives and risk levels.

**QUESTION 55**
Which of the following tools is used to attack the Digital Watermarking?

A. Steg-Only Attack
B. Active Attacks
C. 2Mosaic
D. Gifshuffle

**Answer:** C
**Explanation:**
2Mosaic is a tool used for watermark breaking. It is an attack against a digital watermarking system. In this type of attack, an image is chopped into small pieces and then placed together.

When this image is embedded into a web page, the web browser renders the small pieces into one image. This image looks like a real image with no watermark in it. This attack is successful, as it is impossible to read watermark in very small pieces. Answer: D is incorrect. Gifshuffle is used to hide message or information inside GIF images. It is done by shuffling the colormap. This tool also provides compression and encryption. Answer: B and A are incorrect. Active Attacks and Steg- Only Attacks are used to attack Steganography.

**QUESTION 56**
You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

A. Quantitative risk analysis
B. Qualitative risk analysis
C. Seven risk responses
D. A risk probability-impact matrix

**Answer:** B
**Explanation:**
Qualitative risk analysis is a high-level, fast review of the risk event. Qualitative risk analysis qualifies the risk events for additional analysis.

**QUESTION 57**
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Project Management Information System
B. Integrated Change Control
C. Configuration Management System
D. Scope Verification

**Answer:** C
**Explanation:**
The change management system is comprised of several components that guide the change request through the process. When a change request is made that will affect the project scope. The Configuration Management System evaluates the change request and documents the features and functions of the change on the project scope.

**QUESTION 58**
You work as a project manager for BlueWell Inc. You with your team are using a method or a (technical) process that conceives the risks even if all theoretically possible safety measures would be applied. One of your team member wants to know that what is a residual risk. What will you reply to your team member?

A. It is a risk that remains because no risk response is taken.
B. It is a risk that can not be addressed by a risk response.
C. It is a risk that will remain no matter what type of risk response is offered.
D. It is a risk that remains after planned risk responses are taken.

**Answer:** D
**Explanation:**
Residual risks are generally smaller risks that remain in the project after larger risks have been addressed. The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. This is not a valid statement about residual risks. Answer: C is incorrect. This is not a valid statement about residual risks. Answer: A is incorrect. This is not a valid statement about residual risks.

**QUESTION 59**
You are the project manager of the NNN project for your company. You and the project team are working together to plan the risk responses for the project. You feel that the team has successfully completed the risk response planning and now you must initiate what risk process it is. Which of the following risk processes is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased?

A. Quantitative risk analysis
B. Risk identification
C. Risk response implementation
D. Qualitative risk analysis

**Answer:** A
**Explanation:**
The quantitative risk analysis process is repeated after the plan risk responses to determine if the overall project risk has been satisfactorily decreased. Answer: D is incorrect. Qualitative risk analysis is not repeated after the plan risk response process. Answer: B is incorrect. Risk identification is an ongoing process that happens throughout the project. Answer: C is incorrect. Risk response implementation is not a project management process.

**QUESTION 60**
Which of the following statements is true about residual risks?

A. It is the probabilistic risk after implementing all security measures.
B. It can be considered as an indicator of threats coupled with vulnerability.
C. It is a weakness or lack of safeguard that can be exploited by a threat.
D. It is the probabilistic risk before implementing all security measures.

**Answer:** A
**Explanation:**
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that still conceives these dangers even if all theoretically possible safety measures would be applied. The formula to calculate residual risk is (inherent risk) x (control risk) where inherent risk is (threats vulnerability). Answer: B is incorrect. In information security, security risks are considered as an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. Answer: C is incorrect. Vulnerability is a weakness or lack of safeguard that can be exploited by a threat, thus causing harm to the information systems or networks. It can exist in hardware , operating systems, firmware, applications, and configuration files. Vulnerability has been variously defined in the current context as follows: 1.A security weakness in a Target of Evaluation due to failures in analysis, design, implementation, or operation and such. 2.Weakness in an information system or components (e.g. system security procedures, hardware design, or internal controls that could be exploited to produce an information-related misfortune.) 3.The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the system, network, application, or protocol involved.

**QUESTION 61**
To help review or design security controls, they can be classified by several criteria . One of these criteria is based on their nature. According to this criterion, which of the following controls consists of incident response processes, management oversight, security awareness, and

training?

A. Compliance control
B. Physical control
C. Procedural control
D. Technical control

**Answer:** C
**Explanation:**
Procedural controls include incident response processes, management oversight, security awareness, and training. Answer: B is incorrect. Physical controls include fences, doors, locks, and fire extinguishers. Answer: D is incorrect. Technical controls include user authentication (login) and logical access controls, antivirus software, and firewalls. Answer: A is incorrect. The legal and regulatory, or compliance controls, include privacy laws, policies, and clauses.

**QUESTION 62**
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Trademark law
B. Security law
C. Privacy law
D. Copyright law

**Answer:** C
**Explanation:**
The credit card issuing company has violated the Privacy law. According to the Internet Privacy law, a company cannot provide their customer's financial and personal details to other companies. Answer: A is incorrect. Trademark laws facilitate the protection of trademarks around the world. Answer: B is incorrect. There is no law such as Security law. Answer: D is incorrect. The Copyright law protects original works or creations of authorship including literary, dramatic, musical, artistic, and certain other intellectual works.

**QUESTION 63**
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?

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

**Answer:** A
**Explanation:**
Only acceptance is appropriate for both positive and negative risk events. Often sharing is used for low probability and low impact risk events regardless of the positive or negative effects the risk event may bring the project. Acceptance response is a part of Risk Response planning process.