ISC2

(CGRC)

Certified in Governance, Risk and Compliance

DUMPSGATE

726

Question: 1

An event or situation that has the potential for causing undesirable consequences or impact.
Response:

A. Threat Event
B. Threat Assessment
C. Threat Source
D. Threat Scenario

Answer: A

Question: 2

In which type of access control do user ID and password system come under?
Response:

A. Administrative
B. Technical
C. Power
D. Physical

Answer: B

Question: 3

The Organization Level (Tier 1) strategy addresses/requires.....
Response:

A. *Assessment of Risks
*Evaluation of Risks
*Mitigation of Risks
*Acceptance of Risk
*Monitoring Risk
*Risk Management Strategy Oversight
B. *Mitigation of Risks
*Acceptance of Risk

*Monitoring Risk
*Risk Management Strategy Oversight
* Assessment of Risks
* Evaluation of Risks
C. *Acceptance of Risk
*Assessment of Risks
*Evaluation of Risks
*Mitigation of Risks
*Monitoring Risk
* Risk Management Strategy Oversight
D. *Evaluation of Risks
*Mitigation of Risks
*Acceptance of Risk
*Monitoring Risk
* Assessment of Risks
* Risk Management Strategy Oversight

Answer: A

Question: 4

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.
Response:

A. Adversary
B. Enterprise
C. Countermeasures
D. Assurance

Answer: A

Question: 5

Choose from the following options the U.S. government repository of standards-based vulnerability management data where you can easily find the NIST standards for guidance on continuous monitoring.
Response:

A. NIST SP 800-37
B. NVD
C. SCAP
D. ISCM

Answer: B

Question: 6

In the case of a complex information system, where a “leveraged authorization” that involves two agencies will be conducted, what is the minimum number of system boundaries/accreditation boundaries that can exist?
Response:

A. Only one.
B. Only two, because there are two agencies.
C. At least two.
D. A leveraged authorization cannot be conducted with more that one agency involved.

Answer: A

Question: 7

What is the MOST appropriate action to take after weaknesses or deficiencies in controls are corrected?
Response:

A. The system is given an Authority to Operate (ATO)
B. The remediated controls are reassessed
C. The assessment report is generated
D. The original assessment results are changed

Answer: B

Question: 8

You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating.
You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?
Response:

A. Sharing
B. Avoidance
C. Transference
D. Exploiting

Answer: C

Question: 9

Which of the following are the goals of risk management?
Each correct answer represents a complete solution. Choose three.
Response:

A. Finding an economic balance between the impact of the risk and the cost of the countermeasure
B. Identifying the risk
C. Assessing the impact of potential threats
D. Identifying the accused

Answer: A,B,C

Question: 10

What would be the impact level due to the loss of CIA that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations or the nation?
Response:

A. Low impact level
B. Medium impact level
C. Moderate impact level
D. High impact level

Answer: D

Question: 11

Which of the following is not an authorization decision identified in the RMF?
Response:

A. Authorization to operate
B. Denial of authorization to operate
C. Common control authorization
D. All of the above

Answer: D

Question: 12

Sensitivity of a system based on the_____processed, stored, and transmitted by the system.
Response:

A. Data
B. Program
C. Image
D. Signal

Answer: A

Question: 13

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

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

Answer: D

Question: 14

Where would you find standard guidance for determining an organization's risk appetite?
Response:

A. NIST SP 800-39
B. NIST SP 800-50
C. NIST SP 800-37
D. NIST SP 800-53

Answer: A

Question: 15

The FISMA defines three security objectives for information and information systems:

Response:

A. CONFIDENTIALITY, INTEGRITY and AVAILABILITY
B. INTEGRITY, AVAILABILITY and AUTHENTICITY
C. AVAILABILITY, AUTHENTICITY and CONFIDENTIALITY
D. AUTHENTICITY, CONFIDENTIALITY and INTEGRITY

Answer: A

Question: 16

Which of the following tasks are identified by the Plan of Action and Milestones document?
Each correct answer represents a complete solution. Choose all that apply.
Response:

A. The plans that need to be implemented
B. The resources needed to accomplish the elements of the plan
C. Any milestones that are needed in meeting the tasks
D. The tasks that are required to be accomplished
E. Scheduled completion dates for the milestones

Answer: B,C,D,E

Question: 17

Authentication ensures that system users are who they say the are. At Colvine Tech, a system user must prove identity by providing an email address, a password, and answer a security question before being given logical access
What factor of authentication fits this requirement?
Response:

A. Multi-factor authentication
B. Authentication and accountability
C. Single-factor authentication
D. Dual-factor authentication

Answer: C

Question: 18

The ability to quickly adapt and recover from any known or unknown changes to the environment through holistic implementation of risk management, contingency, and continuity planning.

Response:

A. Resilience
B. Fragile
C. Inanimate
D. Silence

Answer: A

Question: 19

A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.
Response:

A. Disaster Recovery Plan (DRP)
B. Common Vulnerability Scoring System (CVSS)
C. Continuity of Operations Plan (COOP)
D. Common Vulnerability and Exposures (CVE)

Answer: A

Question: 20

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect; a serious adverse effect, or a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Response:

A. Potential Impact
B. High Impact
C. Low Impact
D. Moderate Impact

Answer: A

Question: 21

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?
Response:

A. Safeguards
B. Preventive controls
C. Detective controls
D. Corrective controls

Answer: D

Question: 22

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Response:

A. Authorization (to operate)
B. Systems operated
C. Security Authorization
D. Senior Organizational

Answer: A

Question: 23

Which of the following are the common roles with regard to data in an information classification program?
Each correct answer represents a complete solution. Choose all that apply.
Response:

A. Custodian
B. User
C. Security auditor
D. Editor
E. Owner

Answer: A,B,C,E

Question: 24

What RMF artifact establishes the scope of protection for an IS and encompass people, process, and info tech that are part of the system?

A. Response:
B. System Boundary
C. Risk Management Framework
D. Authorize
E. Categorization

Answer: A

Question: 25

The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States;
(i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).
Response:

A. High Impact
B. Low Impact
C. Medium Impact
D. Moderate Impact

Answer: A

Question: 26

The findings from a security control assessment are documented in which of the following documents?
Response:

A. Security Assessment Plan (SAP)
B. Plan of Action & Milestones (POA&M)
C. Security Assessment Report (SAR)
D. System Security and Privacy Plan

Answer: C

Question: 27

The security control type for an information system that primarily are implemented and executed by people (as opposed to systems).

Response:

A. Operational
B. Technical
C. Organizational
D. Implementation

Answer: A

Question: 28

The security controls for an information system that primarily are implemented by people (as opposed to systems) are known as
Response:

A. Management controls
B. Operational controls
C. Technical controls
D. Logical controls

Answer: B

Question: 29

The authorizing official may determine that additional information supporting the authorization package is needed. The additional documentation may include all but one of the following.
Response:

A. Plan of action and milestones
B. Risk assessments
C. Contingency plans
D. Supply chain risk management plans

Answer: A

Question: 30

A busines-sbased framework for government wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen- centered, results-oriented, and market-based.
Response:

A. Federal Enterprise Architecture
B. Net-Centric Architecture
C. Industry Standard Architecture
D. Enterprise Architecture

Answer: A

Question: 31

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities.
For your project archives, which one of the following is an output of risk monitoring and control?
Response:

A. Quantitative risk analysis
B. Qualitative risk analysis
C. Requested changes
D. Risk audits

Answer: C

Question: 32

Defining the types of information needed by the organization to successfully carry out identified missions and business processes as well as defining the organization's internal and external information flows.
Response:

A. NIST SP 800-60
B. NIST SP 800-57
C. NIST SP 800-50
D. NIST SP 800-37

Answer: A

Question: 33

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.
Response:

A. Security Control Baseline

B. Minimum Security Baselines
C. None of these
D. Revised Control Baseline

Answer: A

Question: 34

The security category of information 1 is determined to be: Confidentiality, low; Integrity, moderate; and availability, Moderate. The security category for information 2 is determined to be: confidentiality, Not Applicable, Integrity, Low; and availability, Moderate. What is the overall security category?
Response:

A. Security Category information type = (confidentiality, NOT APPLICABLE), (integrity, LOW), (availability, MODERATE)
B. Security Category information type = (confidentiality, LOW), (integrity, LOW), (availability, MODERATE)
C. Security Category information type = (confidentiality, NOT APPLICABLE), (integrity, MODERATE), (availability, HIGH)
D. Security Category information type = (confidentiality, LOW), (integrity, MODERATE), (availability, MODERATE)

Answer: D

Question: 35

The emphasis of the revised NIST SP 800-37 process is on.....
Response:

A. Building information security controls into government information systems by applying up-to-date management, operational and technical security controls.
B. Maintaining awareness of the security posture of information systems through the application of "enhanced monitoring processes."
C. Providing senior leaders essential information to facilitate decision making with regard to risk acceptance.
D. Creating secured environment to provide guidance to individuals involved in security information systems
E. Developing leadership to use, analyze and manage technical security of government information systems

Answer: A,B,C

Question: 36

Which of the following is NOT an objective of the security program?
Response:

A. Security plan
B. Security education
C. Security organization
D. Information classification

Answer: A

Question: 37

Certification and Accreditation (C&A or CnA) is a process for implementing information security. Which of the following is the correct order of C&A phases in a DITSCAP assessment?
Response:

A. Definition, Validation, Verification, and Post Accreditation
B. Verification, Definition, Validation, and Post Accreditation
C. Verification, Validation, Definition, and Post Accreditation
D. Definition, Verification, Validation, and Post Accreditation

Answer: D

Question: 38

Prepare, Categorize, select, and implement are steps or phases of the risk management framework which can be described as
Response:

A. The certification phase of the system authorization plan
B. The pre-certification phase of the system authorization plan
C. The authorization phase of the system authorization plan
D. The post-authorization phase of the system authorization plan

Answer: B

Question: 39

A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy -Act and E Government Act to businesses, sole proprietors, aliens, etc.
Response:

A. Individual
B. Combined
C. Private
D. Mixed

Answer: A

Question: 40

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
Response:

A. Authenticity
B. Validity
C. Complexity
D. Responsibility

Answer: A

Question: 41

In which of the following elements of security does the object retain its veracity and is intentionally modified by the authorized subjects?
Response:

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

Answer: A

Question: 42

What is the purpose of a Privacy impact assessment?
Response:

A. To determine the extent to which proposed or actual changes to the system or its environment of operation can affect or have affected the system's security posture
B. To determine the level of impact of the violation of the confidentiality of PII
C. To determine if the information system processes PII
D. To determine the level of voilation of CIA

Answer: B

Question: 43

A discrete set of resources organized for the collection, processing, maintenance, or disposition of information best describes one of the following
Response:

A. An information system
B. General Support System (GSS)
C. An IT infrastructure
D. A Major Application

Answer: A

Question: 44

Who is primarily responsible for the withdrawal and decommissioning of and information system?
Response:

A. Security Architect
B. Senior Information System Security Officer
C. Information System Security Engineer
D. Information System Owner

Answer: D

Question: 45

Tailoring refers to the process by which a security control baseline is modified based on all but one of the following:
Response:

A. The security categorization of the information system
B. The application of scoping guidance

C. The specification of compensating controls
D. The specification of organization-defined parameters in controls via explicit assignement and selection statements.

Answer: A

Question: 46

Which of the following statements about the authentication concept of information security management is true?
Response:

A. It determines the actions and behaviors of a single individual within a system, and identifies that particular individual.
B. It ensures that modifications are not made to data by unauthorized personnel or processes.
C. It establishes the identity of users and ensures that the users are who they say they are.
D. It ensures the reliable and timely access to resources.

Answer: C

Question: 47

What is the first SDLC phase; which maps to the first two RMF steps (Categorization, Select Controls)?
Response:

A. Initiation
B. Categorization
C. Implementation
D. Disposition

Answer: A

Question: 48

True or False; After an ATO is granted, ongoing continuous monitoring is performed on all identified security controls as well as physical environment, etc..
Response:

A. True
B. False

Answer: A

Question: 49

The security control assessor for Colvine Tech will be conducting a comprehensive level assessment on an information system at Colvine Tech. Which controls must be assessed separately, not by the assessor for colvine Tech?
Response:

A. Common Controls
B. Management controls
C. Failed controls
D. Alternative controls

Answer: A

Question: 50

What is the 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.
Response:

A. Certification
B. Examination
C. Operation
D. Information

Answer: A

Question: 51

A security assessment plan comprises of all of the following except one
Response:

A. Scope
B. Methodology
C. Recommendations for remediation
D. Rules of engagement

Answer: C

Question: 52

Which NIST special configuration provides guidance on security-focused configuration management?
Response:

A. NIST SP 800-128
B. NIST SP 800-37
C. NIST SP 800-30
D. NIST SP 800-137

Answer: A

Question: 53

The authorization boundary of a system undergoing assessment comprises of:
Response:

A. The information System (IS) elements to be authorized for operation
B. Any elements or systems specified by the Chief Information Owner (CIO)
C. Any components found withing the given Internet Protocol (IP) range
D. The information System (IS) elements to be authorized for operation as well as interconnected systems

Answer: A

Question: 54

Which of the following BEST describes the objective of a Security Assessment Plan?
Response:

A. It provides a detailed roadmap for how the assessment will be conducted
B. It provides an assessment process for the integration of software and hardware
C. It describes how to verify the change control and Configuration Management (CM) practices
D. It ensures that changes made during system development are included in security assessments.

Answer: A

Question: 55

You are the project manager for a construction project. The project includes a work that involves very high financial risks. You decide to insure processes so that any ill happening can be compensated. Which type of strategies have you used to deal with the risks involved with that particular work?
Response:

A. Transfer
B. Mitigate
C. Accept
D. Avoid

Answer: A

Question: 56

Security categorization of an National Security System must consider the security categories of all information types resident on it.
Response:

A. True
B. False

Answer: A

Question: 57

The Security Category that primarily deals with preserving authorized restrictions on information access and disclosure.
Response:

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

Answer: A

Question: 58

As indicated in NIST SP 800-37, and NIST SP 800-53 the RMF provides architectural description inputs to the risk management strategy, including mission/business processes, FEA reference models, segment and solution architecture and: