Vendor: (ISC)2

Exam Code: CGRC

Exam Name: Certified in Governance Risk and Compliance

Version: DEMO

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: ABC

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: BCDE

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: ABCE

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 business-based 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

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**