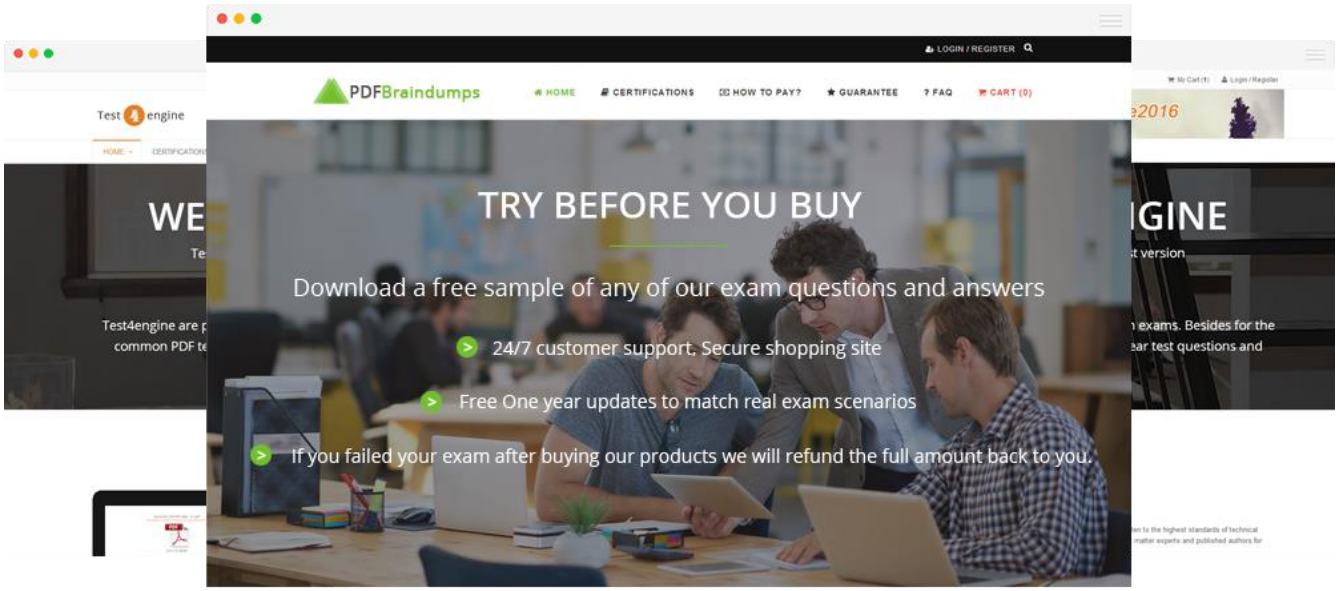
PDFBraindumps



Latest Pdf Braindumps

- LRP-614
- C-SRM-72
- BCABA
- ACMP-6.3
- JN0-740
- 1z0-100
- 250-405
- FM0-308
- DS-200
- C_SRM_72
- SDM_2002001040
- ACMP_6.3
- ST0-250
- 1z0-062
- H12-221
- A4120-784
- M2180-716

Top Certifications

- ISEB Certification
- HCNP
- OCE
- IFPUG Certifications
- NVIDIA Certifications
- dotMobi Certification
- Network+
- SCMA
- IBM Certified Integrat
- MCSD
- CCDH
- NCLP
- IBM Certified Advanc
- XMLMaster Certificat
- eserver Certified Spe
- CS5
- SAP-Certifications
- CHA
- Network Appliance N

Top Vendors

- ISEB
- Fortinet
- ASTQB
- Ericsson
- Aruba
- Liferay
- Data Center Universit
- Novell
- HRCI
- Huawei
- CIW
- RSA
- Patchlink
- MYSQL
- International Consorti
- ISM
- Acme-Packet
- CheckPoint

http://www.pdfbraindumps.com

Latest pdf braindumps provider, high pass rate

Exam : **CGRC**

Title : Certified in Governance Risk and Compliance

Vendor : ISC

Version : DEMO

NO.1 Which SDLC phase can use the System Authorization package to assist with decommissioning tasks for an IS?
Response:
A. Disposition
B. Authorization
C. Operation
D. Remediation
Answer: A

NO.2 An information system's boundary definition resides with who? Response:
A. The Information System Owner, in which he or she would must be careful to consult with authorizing officials (AO), the CIO, CISO, and the risk executive (function)..
B. The Information System Owner, in which he would must be careless to consult with authorizing officials (AO), the CIO, CISO, and the risk executive (function)..
C. The Information System Owner, in which she would must be careful to consult with authorizing officials (AO), the CIO, CISO, and the risk executive (function)..
D. The Information System Owner, in which he or she would must be careful to consult with authorizing officials (AO), the CIO, CISO, and the safe executive (function)..
Answer: A

NO.3 What are the three tools necessary for managing the inventory program? Response:
A. 1. Inventory form.
2. Inventory change form.
3. Organization inventory summary.
B. 1. Inventory change form.
2. Organization inventory summary.
3. Inventory form.
C. 1. Acquisition/Development
2. Inventory change form.
3. Organization inventory summary.
D. 1. Acquisition/Development
2. Organization inventory summary.
3. Inventory change form.
Answer: A

NO.4 This process is used to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates between authorization decisions.
Response:
A. Continuous monitoring
B. Configuration management
C. Vulnerability assessment
D. Certification and accreditation
Answer: A

NO.5 When attempting to categorize a system, which two Risk Management Framework (RMF) starting point inputs should be accounted for?
Response:
A. Federal laws and organizational policies
B. Federal laws and Office of Management and Budget (OMB) policies
C. Federal Information Security Management Act (FISMA) and the Privacy Act
D. Architectural descriptions and organizational inputs
Answer: D

NO.6 What is the potential impact if the loss of confidentiality, integrity, or availability 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?
Response:
A. Low
B. Moderate
C. Severe
D. High
Answer: D

NO.7 The Assessment Test plan once developed is submitted to _____ for approval.
Response:
A. Team Lead
B. Guest
C. Host
D. System Owner
Answer: C

NO.8 Who is responsible for reviewing the assessment reports and plans of action and milestones and determining whether the identified risks need to be mitigated prior to authorization? Response:
A. The Common Control Provider (CCP)
B. The Information System Owner (ISO)
C. The Certifying Agent
D. The Authorizing Official
Answer: D

NO.9 According to NIST SP 800-37 Rev 2, step 5 of the risk management framework 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: A

NO.10 Which of the following is used to indicate that the software has met a defined quality level and is ready for mass distribution either by electronic means or by physical media? Response:
A. RTM
B. CRO
C. DAA
D. ATM
Answer: A

NO.11 Any telecommunications system or information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency that (1) the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, involves command and control of military forces; involves equipment that is an integral part of a weapon system; or is critical to the direct to the direct fulfilment of military or (2) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an executive order or an act of congress is:
Response:
A. Critical system
B. National security system
C. Information system
D. System
Answer: B

NO.12 The test plan should evaluate plans that support the IS; such as Incident Response, Disaster Recovery, and _____ Plan to ensure they are up to date & meet the protection needs of the system Response:
A. Contingency Plan
B. Security Plan
C. Assessment Plan
D. Remediation plan
Answer: A

NO.13 Which RMF role needs to be aware of id of new threats, evolving risks, changes in data sensitivity/criticality and changes in operating environment; to make conscious decision on whether system needs to re-certify.
Response:
A. Authorizing Official (AO)
B. Polar Ozone and Aerosol Measurement (POAM)
C. Industry Standard Architecture (ISA)
D. Superintendent of Police (SP)
Answer: A

NO.14 The ability of an information system to continue to: (i) operate under adverse conditions or

stress, even if in a degraded or debilated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
Response:
A. Information System Resilience
B. Information System Owner
C. Authorizing Official
D. Large Scale Integration
Answer: A

NO.15 Which of the following parts of BS 7799 covers risk analysis and management? Response:
A. Part 1
B. Part 3
C. Part 2
D. Part 4
Answer: B

NO.16 When should the assessment team provide the briefing following the conclusion of testing to provide system management/operations personnel an opportunity to know the security posture and take immediate actions; 24 hrs, 48 hrs, immediately)?
Response:
A. Immediately
B. 24 hrs
C. 48 hrs
D. Later
Answer: A

NO.17 Which of the following NIST documents includes components for penetration testing?
Response:
A. NIST SP 800-53
B. NIST SP 800-26
C. NIST SP 800-37
D. NIST SP 800-30
Answer: D

NO.18 What are the 2 activities involved in certification testing? Response:
A. Assessment of controls, Documentation of Results
B. Assessment of controls
C. Security Controls Assessment
D. Security Controls Assessment, Documentation of Results
Answer: A

NO.19 An analysis of how information is handled:
1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding

privacy;
2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and
3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Response:

A. Privacy Impact Assessment (PIA)

B. Core Nodal Switching Subsystem (CNSS)

C. Industry Standard Architecture (ISA)

D. Personally Identifiable Information (PII)

Answer: A

NO.20 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? Response:

A. Security law

B. Privacy law

C. Copyright law

D. Trademark law

Answer: B

NO.21 Which of the following components ensures that risks are examined for all new proposed change requests in the change control system?
Response:

A. Risk monitoring and control

B. Scope change control

C. Configuration management

D. Integrated change control

Answer: D

NO.22 Managing information security risk from an organization-wide perspective has to do with the following processes except one. Choose the exception.
Response:

A. responding to rist

B. Framing risk

C. Assessing risk

D. Mitigating risk

Answer: D

NO.23 Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life? Response:

A. Configuration management

B. Procurement management
C. Risk management
D. Change management
Answer: A

NO.24 What is NIST SP 800-37 R1?
Response:
A. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach
B. Guide for Applying the Risk Management Framework to Federal Information Systems. A unsecure Life Cycle Approach
C. Guide for Applying the Safe Management Framework to Federal Information Systems. A Security Life Cycle Approach
D. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Unapproachable.
Answer: A

NO.25 Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.
Response:
A. Protect society, the commonwealth, and the infrastructure.
B. Act honorably, honestly, justly, responsibly, and legally.
C. Provide diligent and competent service to principals.
D. Give guidance for resolving good versus good and bad versus baddilemmas.
Answer: ABC

NO.26 Assessment methods have a set of associated attributes which help define the level of effort for the assessment. Which of the following is the right pair of attributes? Response:
A. depth and coverage
B. coverage and scope
C. Breadth and coverage
D. rigor and level of detail
Answer: A

NO.27 What is the name of the formal document that provides an overview of security requirements for the information system and describes the security controls in place or planned for meeting those requirements?
Response:
A. Security Assessment Plan (SAP)
B. Plan of Action & Milestones (POA&M)
C. System Security and Privacy Plan
D. Security Assessment Report (SAR)
Answer: C

NO.28 In what phases of the RMF and SDLC, respectively, does documentation of control implementation start?
Response:
A. Implement Controls & Development/Acquisition
B. Categorization and Initiation
C. Authorization and operations/Maintenance
D. Monitor and Sunset
Answer: A

NO.29 Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in. What are the different categories of penetration testing? Each correct answer represents a complete solution. Choose all that apply.
Response:
A. Full-box
B. Zero-knowledge test
C. Full-knowledge test
D. Open-box
E. Partial-knowledge test
F. Closed-box
Answer: BCDEF

NO.30 The system authorization program often fails due to failure to separate and assign duties at the system level, poor planning, poor systems inventory and many other reasons including which of the following? Response:
A. Inability to work with remote teams.
B. Lack of management support.
C. Lack of project management office.
D. Insufficient system rights.
Answer: B

NO.31 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

NO.32 Which of the following administrative policy controls requires individuals or organizations to

be engaged in good business practices relative to the organization's industry? Response:
A. Segregation of duties
B. Separation of duties
C. Need to Know
D. Due care
Answer: D

NO.33 In which of the 6 steps of RMF is the System Boundary defined? Response:
A. Step 1
B. Step 2
C. Step 3
D. Step 4
Answer: A

NO.34 Which of the following specifies security requirements for federal information and information systems in 17 security-related areas that represent a broad-based, balanced information security program? Response:
A. Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems
B. FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
C. Committee on National Security Systems (CNSS) Instruction No. 1253, Security Categorization and Control Selection for National Security Systems
D. Section 3541 Title 44 U.S.C. Federal Information Security Management Act of 2002
Answer: B

NO.35 True or False. Impacts of changes should be known in advance so that appropriate actions can be taken before vulnerabilities are experienced.
Response:
A. True
B. False
Answer: A