ISC.CGRC.v2024-06-23.q151

Exam Code:	CGRC
Exam Name:	Certified in Governance Risk and Compliance
Certification Provider:	ISC
Free Question Number:	151
Version:	v2024-06-23
# of views:	1007
# of Questions views:	1510
https://www.freepdfdumps.com/ISC.CGRC.v2024-06-23.q151.html	

NEW QUESTION: 1
The transfer of risk is one of the five risk treatment methods pointed out in NIST 800-37 Rev 2.
Choose an example of risk transfer from the following options.
Response:
A. Control inheritance
B. Warranty
C. Control implementation
D. Avoindance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major.
Adequate security for other applications should be provided by security of the systems in which they operate.
Response:
A. Worthless Application
B. Slight Application
C. Major Application
D. Humble Application
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3

A security policy is an overall general statement produced by senior management that dictates what role security plays within the organization. Which of the following are required to be addressed in a well designed policy?
Each correct answer represents a part of the solution. Choose all that apply.
Response:
A. What is being secured?
B. Who is expected to comply with the policy?
C. Where is the vulnerability, threat, or risk?
D. Who is expected to exploit the vulnerability?
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 4
The emphasis of the revised NIST SP 800-37 process is on.....
Response:
A. Providing senior leaders essential information to facilitate decision making with regard to risk acceptance.
B. Developing leadership to use, analyze and manage technical security of government information systems
C. Creating secured environment to provide guidance to individuals involved in security information systems
D. Maintaining awareness of the security posture of information systems through the application of
"enhanced monitoring processes."
E. Building information security controls into government information systems by applying up-to-date management, operational and technical security controls.
Answer: (SHOW ANSWER)

NEW QUESTION: 5
Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.
Response:
A. Contingency Plan
B. Disaster Recovery Plan
C. Incident Response Plan
D. Operations Plan
Answer: (SHOW ANSWER)

NEW QUESTION: 6
A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.

Response:
A. Misgiving Casse
B. Belief Case
C. Diffidence Case
D. Assurance Case
Answer: D (LEAVE A REPLY)

NEW QUESTION: 7
In what phases of the RMF and SDLC, respectively, does documentation of control implementation start?
Response:
A. Authorization and operations/Maintenance
B. Monitor and Sunset
C. Implement Controls & Development/Acquisition
D. Categorization and Initiation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Which of the following professionals is responsible for starting the Certification & Accreditation (C&A) process?
Response:
A. Information system owner
B. Authorizing Official
C. Chief Risk Officer (CRO)
D. Chief Information Officer (CIO)
Answer: (SHOW ANSWER)

NEW QUESTION: 9
A chronological record of system activities, including records of system accesses and operations performed in a given period best defines:
Response:
A. Adequate security
B. Assurance
C. Resilience
D. Audit log
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
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. Authorize

B. Risk Management Framework
C. Response:
D. System Boundary
E. Categorization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
There are seven risks responses that a project manager can choose from. Which risk response is appropriate for both positive and negative risk events?
Response:
A. Acceptance
B. Mitigation
C. Sharing
D. Transference
Answer: (SHOW ANSWER)

NEW QUESTION: 12
A part of a project deals with the hardware work. As a project manager, you have decided to hire a company to deal with all hardware work on the project. Which type of risk response is this?
Response:
A. Transference
B. Mitigation
C. Avoidance
D. Exploit
Answer: (SHOW ANSWER)

NEW QUESTION: 13
Which of the following publications serves as a guide for the selection of security controls?
Response:
A. NIST SP 800-53 and FIPS 200
B. FIPS 199 and NIST SP 800-60
C. Organizational policy and procedures
D. System security plan and security assessment report
Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
The Security Category that primarily deals with ensuring timely and reliable access to information.
Response:
A. Availability

B. Integrity
C. Confidentiality
D. Authenticity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
Where can you find guidance for registering information systems in the organization system inventory? Response:
A. NIST SP 800-38d , Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems
B. NIST SP 800-38b , Revision 2 Guide for Applying the Risk Management Framework to Federal Information Systems
C. NIST SP 800-37, Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems
D. NIST SP 800-30, Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
The physical surroundings in which an information system processes, stores, transmits, or disseminates information is referred to as Response:
A. Information System
B. Environment of Operation
C. Facility
D. IT infrastructure
Answer: (SHOW ANSWER)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 17
One of the following sentences can appropriately help Authorizing Officials and CISOs define an accreditation boundary.
Response:
A. Internal and external systems that are interconnected through the internet.

B. The components of an information system that are under the same management authority
C. The set of system elements comprising the system to be authorized for operation or use
Answer: C (LEAVE A REPLY)

NEW QUESTION: 18
Guarding against improper information modification or destruction, and includes ensuring information non- repudiation and authenticity.
Response:
A. Confidentiality
B. Integrity
C. Availability
D. Authenticity
Answer: (SHOW ANSWER)

NEW QUESTION: 19
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 (LEAVE A REPLY)

NEW QUESTION: 20
Which of the following statements are true about security risks? correct answer represents a complete solution. Choose three.
Response:
A. They are considered an indicator of threats coupled with vulnerability.
B. They can be removed completely by taking proper actions.
C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
D. They can be analyzed and measured by the risk analysis process.
Answer: (SHOW ANSWER)

NEW QUESTION: 21
When attempting to categorize a system which two RMF starting point inputs should be accounted for and are critical input to Categorization?
Response:
A. Federal laws and Office of Management and Budget (OMB) policies
B. Federal Information Security Management Act (FISMA) and the Privacy Act
C. Architectural descriptions and organizational inputs

D. Federal laws and organizational policies
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
What is the purpose for scoping guidance?
Response:
A. To allow senior management to establish and express their guidance on tailoring the security control baseline
B. To establish the high water mark as part of FIPS 199 analysis
C. To establish the organizationally defined security parameters
D. To establish which controls will not be part of the baseline
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Sam is the project manager of a construction project in south Florid
A. Mitigation
B. Active acceptance
C. Avoidance
D. Passive acceptance
E. This area of the United States is prone to hurricanes during certain parts of the year. As part of the project plan Sam and the project team acknowledge the possibility of hurricanes and the damage the hurricane could have on the project's deliverables, the schedule of the project, and the overall cost of the project.
Once Sam and the project stakeholders acknowledge the risk of the hurricane they go on planning the project as if the risk is not likely to happen. What type of risk response is Sam using?
Response:
Answer: (SHOW ANSWER)

NEW QUESTION: 24
An official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system or records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.
Response:
A. System Inventory Process
B. System of Records Notice
C. System Interconnection
D. System of Record
Answer: B (LEAVE A REPLY)

NEW QUESTION: 25
The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assests, or individuals. Thus the potential impact is..
Response:
A. Severe
B. Moderate
C. High
D. Low
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Which plan documents objectives for the security control assessment & details how to conduct such an assessment and records assessment procedures (Security Plan, Assessment Plan, POAM)? Response:
A. Assessment Plan
B. Security Plan
C. POAM
D. Contingency Plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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? Response:
A. Penetration test
B. Paper test
C. Full operational test
D. Walk-through test
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
You are the project manager for the NHH project.
You are working with your project team to examine the project from four different defined perspectives to increase the breadth of identified risks by including internally generated risks.
What risk identification approach are you using in this example?
A. SWOT analysis
B. Root cause analysis
C. Assumptions analysis
D. Influence diagramming techniques

Answer: A (LEAVE A REPLY)
SWOT analysis stands for Strengths, Weaknesses, Opportunities, and Threats.
By examining the project from these four perspectives, including internally generated risks, the project team can increase the breadth of identified risks and gain a comprehensive understanding of potential challenges and opportunities.

NEW QUESTION: 29
Which of the following statements about the availability concept of Information security management is true?
Response:
A. It ensures reliable and timely access to resources.
B. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.
C. It ensures that modifications are not made to data by unauthorized personnel or processes .
D. It determines actions and behaviors of a single individual within a system.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 30
The RMF Step and task where a Continuous Monitoring strategy that monitors the effectiveness of the selected security controls is created.
Response:
A. RMF Step 2, Task 2
B. RMF Step 1, Task 3
C. RMF Step 2, Task 1
D. RMF Step 2, Task 3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
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:
Response:
A. Strategic goals and objectives
B. Information system boundaries
C. Information security requirements
D. Laws, directives and policy guidance
Answer: (SHOW ANSWER)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 32
When an ATO is issued, which of the following roles authoritatively accepts residual risk on behalf of the organization?
Response:
A. Information Owner
B. AO or the AO's designated Representation
C. Authorizing official
D. CISO
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
Security testing conducted from inside the organization's security perimeter.
Response:
A. Internal Security Testing
B. Application Security Testing
C. Web Security Testing
D. Software Security Testing
Answer: (SHOW ANSWER)

NEW QUESTION: 34
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. Vulnerability assessment
B. Configuration management
C. Continuous monitoring
D. Certification and accreditation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
Another term used to refer to a Security Controls Assessment or security review; is?
Response:

A. Security Control
B. Security Test (ST)
C. Evaluation
D. Security Test & Evaluation (ST&E)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
In which of the following elements of security does the object retain its veracity and is intentionally modified by the authorized subjects?
Response:
A. Nonrepudiation
B. Availability
C. Confidentiality
D. Integrity
Answer: D (LEAVE A REPLY)

NEW QUESTION: 37
What is NIST SP 800-37 R1?
Response:
A. Guide for Applying the Safe Management Framework to Federal Information Systems. A Security Life Cycle Approach
B. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach
C. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Unapproachable.
D. Guide for Applying the Risk Management Framework to Federal Information Systems. A unsecure Life Cycle Approach
Answer: B (LEAVE A REPLY)

NEW QUESTION: 38
When attempting to categorize a system, which two Risk Management Framework (RMF) starting point inputs should be accounted for?
Response:
A. Architectural descriptions and organizational inputs
B. Federal laws and Office of Management and Budget (OMB) policies
C. Federal laws and organizational policies
D. Federal Information Security Management Act (FISMA) and the Privacy Act
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39

System Authorization is the risk management process. System Authorization Plan (SAP) is a comprehensive and uniform approach to the System Authorization Process. What are the different phases of System Authorization Plan? Each correct answer represents a part of the solution. Choose all that apply.
Response:
A. Authorization
B. Certification
C. Post-Authorization
D. Pre-certification
E. Post-certification
Answer: (SHOW ANSWER)

NEW QUESTION: 40
The findings from a security control assessment are documented in which of the following documents? Response:
A. Security Assessment Plan (SAP)
B. Security Assessment Report (SAR)
C. Plan of Action & Milestones (POA&M)
D. System Security and Privacy Plan
Answer: (SHOW ANSWER)

NEW QUESTION: 41
One of the inputs to the risk determination task is the employment of risk assessments to provide information that may influence the risk analysis and risk determination. What publication provides guidance on conducting risk assessments?
Response:
A. NIST SP 800-59
B. NIST SP 800-37
C. NIST SP 800-30
D. NIST SP 800-39
Answer: (SHOW ANSWER)

NEW QUESTION: 42
The Software Development Life-Cycle phase that maps to RMF Step 2 (select controls), Task 4, SP Approval?
Response:
A. Mission/business process
B. Development/Acquisition
C. Operation/Maintenance
D. Criticality/Sensitivity
Answer: B (LEAVE A REPLY)

NEW QUESTION: 43
Statements of security capability to: (i) build in additional, but related, functionality to a security control; and/or (ii) increase the strength of the control.
Response:
A. System-Specific Security Control
B. Tailored Security Control Baseline
C. Security Control Inheritance
D. Security Control Enhancements
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Which NIST publication is the Guide to applying RMF in Federal Info Systems a Security Life cycle approach & moved process from four phase certification & accreditation approach to emphasis risk management in a 6 step authorization process.
Response:
A. NIST SP 800-53
B. NIST SP 800-40
C. NIST SP 800-37
D. NIST SP 800-39
Answer: C (LEAVE A REPLY)

NEW QUESTION: 45
The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation and maintenance, and ultimately its disposal that instigates another system initiation best describes Response:
A. System Development Life Cycle (SDLC)
B. Authorization Process
C. Information system
D. IT infrastructure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
What is the publication that has the Minimum Security Requirements for Federal Information and Information Systems.
Response:
A. FIPS PUB 200
B. FIPS PUB 299
C. FIPS PUB 300
D. FIPS PUB 250
Answer: A (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 47
Which of the following is used in the practice of Information Assurance (IA) to define assurance requirements?
Response:
A. Communications Management Plan
B. Parkerian Hexad
C. Classic information security model
D. Five Pillars model
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Which of the following control families belongs to the management class of security controls?
Response:
A. Access Control
B. System & Service Acquisition
C. Media Protection
D. Configuration management
Answer: B (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following BEST describes a government-wide standard for security Assessment and Authorization (A&A) and continuous monitoring for cloud products, which is mandatory for federal agencies and cloud service providers (CSP)?
Response:
A. Trusted Computer System Evaluation (TCSEC)
B. Federal Information Technology Acquisition Reform Act (FITARA)
C. National Institute of Standard and Technology (NIST)
D. Federal Risk and Authorization Management Program (FedRAMP)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
What is the three-tiered approach to risk management described in NIST SP 800-37, Revision 1?
Response:
A. Addresses/Requires (Tier 1),
Mission/Business Process Level (Tier 2)
Information System Level (Tier 3)
B. Organization Level (Tier 1),
Mission/Business Process Level (Tier 2)
Information System Level (Tier 3)
C. Organization Level (Tier 1),
Addresses/Requires (Tier 2)
Information System Level (Tier 3)
D. Mission/Business Process Level (Tier 1),
Information System Level (Tier 2)
Organization Level (Tier 3)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 51
Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.
Response:
A. Threat Assessment
B. Threat Source
C. Threat Scenario
D. Threat Event
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Which of the following describes residual risk as the risk remaining after risk mitigation has occurred? Response:
A. DAA
B. ISSO
C. DIACAP
D. SSAA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 53
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. Continuity of Operations Plan (COOP)
B. Common Vulnerability Scoring System (CVSS)
C. Disaster Recovery Plan (DRP)
D. Common Vulnerability and Exposures (CVE)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
FIPS 199, Standards for Security Categorization of Federal Systems defines which 3 Security Categories? Response:
A. Familiarity, Sensitivity, Criticality
B. Architectural descriptions & Organizational
C. Confidentiality, Integrity, Availability
D. Sensitivity, Criticality, availability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 55
What is included in a POA&M that is presented to the Approving Authority as part of the initial authorization package?
Response:
A. Deficiencies that have not yet been remediated and verified throughout the RMF process
B. All failed controls identified throughout the RMF process
C. Only volatile findings that require prioritization in remediation
D. Only findings that have been evaluated as moderate or high
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
James work as an IT systems personnel in SoftTech Inc. He performs the following tasks:
- Runs regular backups and routine tests of the validity of the backup data.
- Performs data restoration from the backups whenever required.
- Maintains the retained records in accordance with the established information classification policy.
What is the role played by James in the organization?
Response:
A. Manager
B. Owner
C. User
D. Custodian
Answer: (SHOW ANSWER)

NEW QUESTION: 57

As indicated in NIST SP 800-37, and NIST SP 800-53 the RMF provides inputs to the risk management strategy, including: laws, directives, and policy guidance; strategic goals and objectives; information security requirements; and:
Response:
A. Segment and solution architecture
B. Priorities and resources availability
C. Mission/business processes
D. FEA reference models
Answer: (SHOW ANSWER)

NEW QUESTION: 58
Which NIST special configuration provides guidance on security-focused configuration management? Response:
A. NIST SP 800-30
B. NIST SP 800-137
C. NIST SP 800-128
D. NIST SP 800-37
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
The Organization Level (Tier 1) strategy addresses/requires.....
Response:
A. *Evaluation of Risks
*Mitigation of Risks
*Acceptance of Risk
*Monitoring Risk
*Assessment of Risks
*Risk Management Strategy Oversight
B. *Acceptance of Risk
*Assessment of Risks
*Evaluation of Risks
*Mitigation of Risks
*Monitoring Risk
*Risk Management Strategy Oversight
C. *Mitigation of Risks
*Acceptance of Risk
*Monitoring Risk
*Risk Management Strategy Oversight
*Assessment of Risks
*Evaluation of Risks
D. *Assessment of Risks

*Evaluation of Risks
*Mitigation of Risks
*Acceptance of Risk
*Monitoring Risk
*Risk Management Strategy Oversight
Answer: (SHOW ANSWER)

NEW QUESTION: 60
Applying the first three steps in the RMF to legacy systems can be viewed in what way to determine if the necessary and sufficient security controls have been appropriately selected and allocated? Response:
A. Level of effort
B. Sequential
C. Gap analysis
D. Common control
Answer: (SHOW ANSWER)

NEW QUESTION: 61
At which point in the Risk Management Framework (RMF) process is a system analyzed for changes that impact the security and privacy posture of the system?
Response:
A. Assess
B. Select
C. Monitor
D. Implement
Answer: C (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 62
FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. Which of the following FITSAF levels shows that the procedures and controls have been implemented?
Response:

A. Level 5
B. Level 4
C. Level 3
D. Level 2
E. Level 1
Answer: (SHOW ANSWER)

NEW QUESTION: 63
A predetermined set of instructions or procedures that describe how an organization's mission essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
Response:
A. Operations Plan
B. Continuity of Operations Plan (COOP)
C. Disaster Recovery Plan
D. Incident Response Plan
Answer: (SHOW ANSWER)

NEW QUESTION: 64
The security assessment plan is prepared to provide the Authorizing Official and other organizational officials with a plan of how the security assessment will be conducted.
Which roles have the primary responsibility to prepare the security assessment plan?
Response:
A. Authorizing official (AO), Authorizing Official Designated Representative (AODR), Security Control Assessor (SCA)
B. Authorizing official (AO), Information System Owner (ISO), Security Control Assessor (SCA)
C. Information System Owner (ISO), Security Control Assessor (SCA), Information System Security Officer (ISSO)
D. Authorizing official (AO), Authorizing Official Designated Representative (AODR), Information System Owner (ISO)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 65
Updating the security plan, security assessment report, and POAM based on results of the continuous monitoring process is what task in RMF Step 6, Monitor.
Response:
A. Task 1, key updates
B. Task 2, key updates
C. Task 3, key updates
D. Task 4, key updates

Answer: (SHOW ANSWER)

NEW QUESTION: 66
Which of the following is not a part of Identify Risks process? Response:
A. Decision tree diagram
B. Influence diagram
C. Cause and effect diagram
D. System or process flow chart
Answer: A (LEAVE A REPLY)

NEW QUESTION: 67
What are the phases of the System Development Life Cycle? Response:
A. 1. Initiation
2. Disposition
3. Implementation
4. Acquisition/Development
5. Initiation
B. 1. Acquisition/Development
2. Implementation
3. Operations/maintenance
4. Disposition
5. Initiation
C. 1. Initiation
2. Acquisition/Development
3. Implementation
4. Operations/maintenance
5. Disposition
D. 1. Implementation
2. Operations/maintenance
3. Disposition
4. Acquisition/Development
5. Initiation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 68
An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
Response:
A. Business Recovery/Disruption Plan (BRP)
B. Disaster Recovery Plan (DRP)

C. Business Impact Analysis (BIA)
D. Business Continuity Plan (BCP)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
When carrying out ongoing risk response, the effectiveness of new, modified, enhanced, or added controls must be...
Response:
A. Verified
B. Tested
C. Examined
D. Reassessed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
Publication that specifies security requirements for federal information and Info Systems in 17 security related areas that represent a broad-based, balanced information security program.
Response:
A. FIPS 299
B. FIPS 200
C. FIPS 199
D. FIPS 300
Answer: (SHOW ANSWER)

NEW QUESTION: 71
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. Systems operated
B. Senior Organizational
C. Authorization (to operate)
D. Security Authorization
Answer: C (LEAVE A REPLY)

NEW QUESTION: 72
What is the 2nd SDLC phase; which maps to the RMF steps 3 & 4 (Implement, Assess)?
Response:

A. Mission/business process
B. Operation/Maintenance
C. Development/Acquisition
D. Criticality/Sensitivity
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
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. Corrective controls
B. Preventive controls
C. Safeguards
D. Detective controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
Who has primary responsibility to develop a report of the results of the security and privacy control assessments, including recommendations for correcting deficiencies in the implemented controls? Response:
A. Security Control Assessor (SCA)
B. Common Control Provider (CCP)
C. Information System Security Officer (ISSO)
D. Information System Owner (ISO)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 75
The security control type for an information system that primarily are implemented and executed by people (as opposed to systems).
Response:
A. Technical
B. Organizational
C. Operational
D. Implementation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 76
What is BRM?
Response:
A. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the month to month business operations of the federal government. The

BRM is the last layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.
B. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the last layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.
C. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the first layer of the Federal Enterprise Architecture (FEA) and provides a bad viewpoint from which to analyze data or service components or technology.
D. The Business Reference Model (BRM) provides an organized, hierarchical framework for describing the day-to-day business operations of the federal government. The BRM is the first layer of the Federal Enterprise Architecture (FEA) and provides a good viewpoint from which to analyze data, service components, and technology.
Answer: D (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 77
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. Open-box
B. Full-knowledge test
C. Full-box
D. Closed-box
E. Partial-knowledge test
F. Zero-knowledge test
Answer: A,B,D,E,F (LEAVE A REPLY)

NEW QUESTION: 78

Which RMF role establishes risk management roles and responsibilities and provides advice and relevant information to authorizing officials concerning the risk management strategy to guide authorization decision making.
Response:
A. Risk executive
B. ISSE
C. System owner
D. Common control provider
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following parts of BS 7799 covers risk analysis and management? Response:
A. Part 3
B. Part 4
C. Part 1
D. Part 2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
Which NIST SP series document is concerned with continuous monitoring for federal information systems and organizations?
Response:
A. SP 800-26
B. SP 800-137
C. SP 800-144
D. SP 800-64
Answer: B (LEAVE A REPLY)

NEW QUESTION: 81
Fill in the blank with an appropriate word. _____ ensures that the information is not disclosed to unauthorized persons or processes.
Solution: Confidentiality
Determine whether the given solution is correct?
Response:
A. Correct
B. Incorrect
Answer: A (LEAVE A REPLY)

NEW QUESTION: 82

Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
Response:
A. Operations Plan
B. Security Controls
C. Contingency Plan
D. Configuration Control
Answer: D (LEAVE A REPLY)

NEW QUESTION: 83
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. Privacy law
B. Copyright law
C. Security law
D. Trademark law
Answer: A (LEAVE A REPLY)

NEW QUESTION: 84
Tom is the project manager for his organization. In his project he has recently finished the risk response planning. He tells his manager that he will now need to update the cost and schedule baselines. Why would the risk response planning cause Tom the need to update the cost and schedule baselines? Response:
A. New or omitted work as part of a risk response can cause changes to the cost and/or schedule baseline.
B. Risk responses protect the time and investment of the project.
C. Risk responses may take time and money to implement.
D. Baselines should not be updated, but refined through versions.
Answer: (SHOW ANSWER)

NEW QUESTION: 85
The primary responsibility to select control assessors rests on which roles? Response:
A. Authorizing offical (AO), Information System Owner (ISO)
B. Information System Owner (ISO), Security Control Assessor (SCA)
C. Authorizing offical (AO), Authorizing Official Designated Representative (AODR)
D. Authorizing Official (AO) and Information System Security Officer (ISSO)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 86
Test Results should be shown as "meeting standards" or "not meeting standards"; or in short

_____, _____.
Response:
A. Pass, fail
B. Yes, no
C. Good, bad
D. True, false
Answer: (SHOW ANSWER)

NEW QUESTION: 87
_____ management offers a structured approach to managing, approving, and documenting changes affecting an IS; critical to continuous assessment of security posture of IS.
Response:
A. Operation
B. Configuration
C. Organization
D. Information
Answer: B (LEAVE A REPLY)

NEW QUESTION: 88
What roles and responsibilities can only be occupied by a government employee?
Response:
A. Risk Executive
Risk Mitigation
Risk Assessment
Authorizing Official (AO)
B. Risk Executive
Chief Information Officer (CIO)
Senior Information Security Officer (SO)
Authorizing Official (AO)
C. Chief Information Officer (CIO)
Senior Information Security Officer (SISO)
Authorizing Official (AO)
Risk Executive
D. Risk Executive
Chief Information Officer (CIO)
Senior Information Security Officer (SISO)

Authorizing Official (AO)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 89
Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Response:
A. Control Baseline
B. Subsystem
C. Safeguards
D. Tailored Security
Answer: (SHOW ANSWER)

NEW QUESTION: 90
The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
Response:
A. Operational Controls
B. Visual controls
C. Embedded controls
D. Common Control
Answer: A (LEAVE A REPLY)

NEW QUESTION: 91
The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Response:
A. Scoping
B. Tailoring
C. Guidance
D. Feature
Answer: (SHOW ANSWER)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com

CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 92
Where can a project manager find risk-rating rules?
Response:
A. Enterprise environmental factors
B. Risk probability and impact matrix
C. Organizational process assets
D. Risk management plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 93
For which of the following reporting requirements are continuous monitoring documentation reports used?
Response:
A. FBI
B. HIPAA
C. FISMA
D. NIST
Answer: C (LEAVE A REPLY)

NEW QUESTION: 94
Which of the three-tiered approaches to risk management address risk at an Enterprise-wide perspective?
Response:
A. Categorization
B. Authorization
C. Organizational
D. Initiation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 95
Which of the following professionals plays the role of a monitor and takes part in the organization's configuration management process?
Response:
A. Common Control Provider
B. Senior Agency Information Security Officer
C. Chief Information Officer

D. Authorizing Official
Answer: (SHOW ANSWER)

NEW QUESTION: 96
During which Risk Management Framework (RMF) step is the system security plan initially approved? Response:
A. RMF Step 3 Implement Security Controls
B. RMF Step 5 Authorize Information System
C. RMF Step 1 Categorize Information System
D. RMF Step 2 Select Security Controls
Answer: D (LEAVE A REPLY)

NEW QUESTION: 97
A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.
Response:
A. Summative
B. Interview
C. Formative
D. Interim
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
Who is primarily responsible for categorizing the Information System? Response:
A. Information system owner
B. System architect
C. IS program manager
D. CIO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 99
Interrelationships of system authorization processes.
Response:
A. 1. Coordinate Security for Interconnected Systems.
2. Apply Minimum Security Baselines.
3. Assess Risk
4. Develop Security Procedures
5. Document the Accreditation Decision
6. System Inventory Process.

7. Create System Authorization Documentation
8. Develop System Security Plan
9. Conduct Certification Testing
10. System Security Authorization Project Planning.

B. 1. Conduct Certification Testing
2. Plan for Remediation
3. Create System Authorization Documentation
4. Document the Accreditation Decision
5. System Inventory Process.
6. Coordinate Security for Interconnected Systems.
7. Assess Risk
8. Develop System Security Plan
9. System Security Authorization Project Planning.
10. Apply Minimum Security Baselines.

C. 1. System Security Authorization Project Planning.
2. System Inventory Process.
3. Assess Sensitivity and Criticality
4. Develop System Security Plan
5. Coordinate Security for Interconnected Systems.
6. Apply Minimum Security Baselines.
7. Assess Risk
8. Develop Security Procedures
9. Conduct Certification Testing
10. Plan for Remediation
11. Create System Authorization Documentation
12. Document the Accreditation Decision

D. 1. System Security Authorization Project Planning.
2. System Inventory Process.
3. Assess Sensitivity and Criticality
4. Develop System Security Plan
5. Create System Authorization Documentation
6. Document the Accreditation Decision
7. Assess Risk
8. Apply Minimum Security Baselines.
9. Develop Security Procedures
10. Conduct Certification Testing
11. Coordinate Security for Interconnected Systems.
12. Plan for Remediation

Answer: C (LEAVE A REPLY)

NEW QUESTION: 100

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. Change management
B. Procurement management
C. Risk management
D. Configuration management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 101
The Security Category that guards against the improper modification or destruction of information and includes ensuring information non-repudiation & authenticity.
Response:
A. Confidentiality
B. Integrity
C. Authenticity
D. Availability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102
What publication provides an approach for performing system-level risk assessments?
Response:
A. NIST SP 800-60
B. NIST SP 800-39
C. NIST SP 800-30
D. NIST SP 800-50
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Why is the early selection of assessors important to organizations implementing a systems security engineering approach?
Response:
A. Early selection of assessors voilates security requirements
B. Early selection of assessors complete security control assessments in a timely manner
C. Early selection of assessors support verification and validation activities that occur throughout the system life cycle
D. Early selection of assessors assess all implement security controls
Answer: C (LEAVE A REPLY)

NEW QUESTION: 104

During the assessment of security controls, some failed controls (quick fixes) may be remediated immediately or before the final security assessment report is completed and submitted in the ATO package. These controls must be...
Response:
A. Documented in the interim SAR
B. Document in the final SAR
C. Entered in the POA&M
D. Reassessed and documended.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 105
Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?
Response:
A. Employees
B. Hackers
C. Visitors
D. Customers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 106
You are the project manager for your company and a new change request has been approved for your project. This change request, however, has introduced several new risks to the project. You have communicated these risk events and the project stakeholders understand the possible effects these risks could have on your project.
You elect to create a mitigation response for the identified risk events. Where will you record the mitigation response?
Response:
A. Risk log
B. Risk management plan
C. Risk register
D. Project management plan
Answer: C (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here:

https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 107
All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected best defines:
Response:
A. Network Boundary
B. System Boundary
C. Creditation Boundary
D. Authorization Boundary
Answer: (SHOW ANSWER)

NEW QUESTION: 108
When does monitoring security controls take place?
Response:
A. Before and after the initial system security accreditation
B. After the initial system security authorization
C. During the system design phase
D. Before the initial system certification
Answer: (SHOW ANSWER)

NEW QUESTION: 109
Wendy is about to perform qualitative risk analysis on the identified risks within her project. Which one of the following will NOT help Wendy to perform this project management activity?
Response:
A. Project scope statement
B. Risk register
C. Risk management plan
D. Stakeholder register
Answer: D (LEAVE A REPLY)

NEW QUESTION: 110
Which of the following NIST documents includes components for penetration testing?
Response:
A. NIST SP 800-26
B. NIST SP 800-53
C. NIST SP 800-30
D. NIST SP 800-37

Answer: C (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following DoD directives is referred to as the Defense Automation Resources Management Manual?
Response:
A. DoD 7950.1-M
B. DoD 5200.22-M
C. DoD 8910.1
D. DoDD 8000.1
E. DoD 5200.1-R
Answer: (SHOW ANSWER)

NEW QUESTION: 112
You and your project team are identifying the risks that may exist within your project. Some of the risks are small risks that won't affect your project much if they happen. What should you do with these identified risk events?
Response:
A. All risks must have a valid, documented risk response
B. These risks can be accepted
C. These risks can be added to a low priority risk watch list
D. These risks can be dismissed
Answer: (SHOW ANSWER)

NEW QUESTION: 113
Who makes decision to require an IS to under re-accreditation based on security status reporting
& documentation & recommendation of Designated Rep & IT security staff? Response:
A. Industry Standard Architecture (ISA)
B. Authorizing Official (AO)
C. Information Systems Security Officer (ISSO)
D. Information System Owner (ISO)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 114
Which of the following individuals is responsible for preparing and submitting security status reports to the organizations?
Response:
A. Senior Agency Information Security Officer
B. Chief Information Officer
C. Authorizing Official

D. Common Control Provider
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
An initial remediation action was taken by the information system owner (ISO) based on findings from the security assessment report (SAR). What is the next appropriate step based on the Risk Management Framework (RMF)?
Response:
A. ISO documents the remedial action in the security plan.
B. Remedial action taken is sent for review to the ISSO.
C. Include the remediation action taken by information system owner as an addendum to the SAR.
D. Information system security officer (ISSO) documents the remediation action and informs the ISO.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 116
Which of the following are included in Administrative Controls? Each correct answer represents a complete solution. Choose all that apply.
Response:
A. Developing policy
B. Implementing change control procedures
C. Conducting security-awareness training
D. Screening of personnel
E. Monitoring for intrusion
Answer: (SHOW ANSWER)

NEW QUESTION: 117
The registration of the system directly follows which RMF task? Response:
A. Task P-17 Requirements allocation
B. Categorize the system
C. Review and approve the SSP
D. Select security controls
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
The purpose of security controls testing is to evaluate the _____ of the security controls protecting an information system.
Response:
A. Powerlessness
B. Effectiveness

C. Potent
D. Inefficacious
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
Although system authorization is important; obtaining ATO is not the end; continuous monitoring provides _____ that an information system remains secure following accreditation.
Response:
A. Anxiety
B. Assurance
C. Assumption
D. All of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 120
An organization's information systems are a mix of Windows and UNIX systems located in a single computer room. Access to the computer room is restricted by the use of door locks that require proximity cards and personal identification numbers (PINs). Only a small percentage of the organizations employees have access to the computer room. The computer room access restriction is an example of what type of security control relative to the hardware in the computer room?
Response:
A. Technical
B. Managerial
C. Inherited
D. System specific
Answer: (SHOW ANSWER)

NEW QUESTION: 121
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.
Response:
A. Certification is a comprehensive assessment of the management, operational, and technical security controls inan information system.
B. Certification is the official management decision given by a senior agency official to authorize operation of an information system.

C. Accreditation is the official management decision given by a senior agency official to authorize operation of an information system.
D. Accreditation is a comprehensive assessment of the management, operational, and technical security controls in an information system.
Answer: (SHOW ANSWER)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 122
Which of the following NIST Special Publication documents provides a guideline on network security testing?
Response:
A. NIST SP 800 42
B. NIST SP 800 53
C. NIST SP 800 37
D. NIST SP 800 53A
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following are the tasks performed by the owner in the information classification schemes? Each correct answer represents a part of the solution. Choose three.
Response:
A. To delegate the responsibility of the data safeguard duties to the custodian.
B. To perform data restoration from the backups whenever required.
C. To review the classification assignments from time to time and make alterations as the business requirements alter.
D. To make original determination to decide what level of classification the information requires, which is based on the business requirements for the safety of the data.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 124

Neil works as a project manager for SoftTech Inc. He is working with Tom, the COO of his company, on several risks within the project. Tom understands that through qualitative analysis Neil has identified many risks in the project.
Tom's concern, however, is that the priority list of these risk events are sorted in "high-risk,"
"moderate-risk," and "low-risk" as conditions apply within the project. Tom wants to know that is there any other objective on which Neil can make the priority list for project risks.
What will be Neil's reply to Tom?
Response:
A. Risks may be listed by categories
B. Risks may be listed by priority separately for schedule, cost, and performance
C. Risk may be listed by the responses in the near-term
D. Risks may be listed by the additional analysis and response
Answer: B (LEAVE A REPLY)

NEW QUESTION: 125
How many steps are in the Risk Management Framework (RMF)? Response:
A. 8
B. 5
C. 7
D. 6
Answer: D (LEAVE A REPLY)

NEW QUESTION: 126
BS 7799 is an internationally recognized ISM standard that provides high level, conceptual recommendations on enterprise security. BS 7799 is basically divided into three parts.
Which of the following statements are true about BS 7799? Each correct answer represents a complete solution. Choose all that apply.
Response:
A. BS 7799 Part 2 was adopted by ISO as ISO/IEC 27001 in November 2005.
B. BS 7799 Part 1 was a standard originally published as BS 7799 by the British Standards Institute (BSI) in 1995.
C. BS 7799 Part 1 was adopted by ISO as ISO/IEC 27001 in November 2005.
D. BS 7799 Part 3 was published in 2005, covering risk analysis and management.
Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 127
An Authorizing Official plays the role of an approver. What are the responsibilities of an Authorizing Official?
Each correct answer represents a complete solution. Choose all that apply.
Response:

A. Ascertaining the security posture of the organization's information system
B. Reviewing security status reports and critical security documents
C. Determining the requirement of reauthorization and reauthorizing information systems when required
D. Establishing and implementing the organization's continuous monitoring program
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 128
One of the following is a formal document that provides an overview of the security requirements for the information system, describes the system and the security controls in place or planned for meeting those requirements.
Response:
A. Security Plan (SP)
B. Plan of Action and Milestones (POA&M)
C. Security and Privacy assessment reports
D. Initial Risk Assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 129
What are the three classifications for security controls for information systems? Response:
A. System-Custom Controls.
Regular Controls.
Hybrid Controls.
B. System-Security Controls.
Common Controls.
Hybrid Controls.
C. System-Specific Controls.
Common Controls.
Hybrid Controls.
D. System-Common Controls.
Regular Controls.
Hybrid Controls.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 130
Which of the following acts is used to recognize the importance of information security to the economic and national security interests of the United States?
Response:
A. Computer Fraud and Abuse Act
B. Lanham Act
C. Computer Misuse Act

D. FISMA
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131
Testing officials should use which NIST publication as guide for developing test procedures?
Response:
A. NIST SP 800-53
B. NIST SP 800-53A
C. NIST SP 800-39
D. NIST SP 800-37A
Answer: B (LEAVE A REPLY)

NEW QUESTION: 132
A planning estimate for the amount of days that it takes to assess a Moderate system is ___ - ___ days.
Response:
A. 4-7
B. 3-6
C. 5-7
D. 3-5
Answer: (SHOW ANSWER)

NEW QUESTION: 133
Which NIST SP details how RMF can be integrated into the System Development Life-Cycle (SDLC)? Response:
A. NIST SP 800-53
B. NIST SP 800-37A
C. NIST SP 800-37
D. NIST SP 800-39
Answer: C (LEAVE A REPLY)

NEW QUESTION: 134
The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.
Response:
A. Potential Impact
B. Impact Result
C. Impact Value
D. None
Answer: C (LEAVE A REPLY)

NEW QUESTION: 135
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Response:
A. Security Controls
B. Hybrid Controls
C. Configuration Controls
D. System-Specific Control
Answer: (SHOW ANSWER)

NEW QUESTION: 136
Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Response:
A. Information Security Policy
B. Information System Owner
C. National Security System
D. System Security Authorization
Answer: A (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 137
A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario.
This best defines a...
Response:
A. Resolution Exercise
B. Flexibility Exercise.

C. Tabletop Exercise
D. Strength Exercise
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.
Response:
A. Network Monitor
B. Hacking Sniffing
C. Network Sniffing
D. Packet Sniffing
Answer: (SHOW ANSWER)

NEW QUESTION: 139
The level of assessor independence is determined based on applicable laws, executive orders, directives, regulations, policies, or standards. Who determines the level of assessor independence? Response:
A. The Ifnormation System Owner (ISO)
B. The Information Owner (IO)
C. The Authorizing Official
D. The Common Control Provider (CCP)
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
What may Colvine Tech do if they determine that the root cause of an unauthorized change is an adversarial attack?
Response:
A. Adjust intrusion detection and prevention system
B. Invoke incident response
C. Implement additional controls to reduce the risk of future attacks
D. All of the above
Answer: D (LEAVE A REPLY)

NEW QUESTION: 141
A SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity.
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: B (LEAVE A REPLY)

NEW QUESTION: 142
The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption.
Response:
A. Business Impact Analysis (BIA)
B. Business Continuity Plan (BCP)
C. Business Recovery/Disruption Plan (BRP)
D. Common Vulnerability and Exposures (CVE)
Answer: B (LEAVE A REPLY)

NEW QUESTION: 143
What are five primary roles associated with the system authorization program? Response:
A. 1. CISO (Chief Information Security Officer or senior information security officer)
2. System Owner
3. ISSO (Information System Security Officer)
4. Certifying Agent (or security control assessor)
5. AO (Approving Authority or authorizing official)
B. 1. ISSO (Information System Security Officer)
2. Certifying Agent (or security control assessor)
3. AO (Approving Authority or authorizing official)
4. CISO (Chief Information Security Officer or senior information security officer)
5. System Owner
C. 1. System Owner
2. ISSO (Information System Security Officer)
3. Certifying Agent (or security control assessor)
4. AO (Approving Authority or authorizing official)
5. CISO (Chief Information Security Officer or senior information security officer)
D. 1. CISO (Chief Information Security Officer or senior information security officer)
2. System Owner
3. ISSO (Information System Security Officer)
4. System Owner
5. Certifying Agent (or security control assessor)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 144

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. Mitigating risk
C. Framing risk
D. Assessing risk
Answer: B (LEAVE A REPLY)

NEW QUESTION: 145
An information system is currently in the initiation phase of the system development life cycle (SDLC) and has been categorized high impact. The information system owner wants to inherit common controls provided by another organizational information system that is categorized moderate impact. How does the information system owner ensure that the common controls will provide adequate protection for the information system?
Response:
A. Perform rigorous testing of the common controls to determine if they provide adequate protection.
B. Ask the common control provider for the system security plan for the common controls.
C. Supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system.
D. Consult with the information system security engineer and the information security architect.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 146
During information system continuous monitoring you have to monitor changes in the machine elements of the system such as computer elements and data stored in hardware - typically in read only memory (ROM) or programmable read only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
What is the name of such and element?
Response:
A. Application
B. Software
C. Hardware
D. Firmware
Answer: D (LEAVE A REPLY)

NEW QUESTION: 147

Gary is the project manager for his project. He and the project team have completed the qualitative risk analysis process and are about to enter the quantitative risk analysis process when Mary, the project sponsor, wants to know what quantitative risk analysis will review. Which of the following statements best defines what quantitative risk analysis will review? Response:
A. The quantitative risk analysis process will analyze the effect of risk events that may substantially impact the project's competing demands.
B. The quantitative risk analysis seeks to determine the true cost of each identified risk event and the probability of each risk event to determine the risk exposure.
C. The quantitative risk analysis reviews the results of risk identification and prepares the project for risk response management.
D. The quantitative risk analysis process will review risk events for their probability and impact on the project objectives.
Answer: (SHOW ANSWER)

NEW QUESTION: 148
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. DAA
B. CRO
C. RTM
D. ATM
Answer: (SHOW ANSWER)

NEW QUESTION: 149
NIST SP 800-64 Rev 2 has been withdrawn but security professionals can still find guidance on system development lifecycle in which Publication?
Response:
A. NIST SP 800-60
B. NIST SP 800-160
C. NIST SP 800-53
D. NIST SP 800-59
Answer: B (LEAVE A REPLY)

NEW QUESTION: 150
The authorization decision may carry restrictions on system operation and caveats that must be followed to maintain the authorization, and other information as determined by the organization including:
Response:
A. Events that may trigger a review of the authorization decision

B. Terms and conditions for the authorization
C. The impact level supported by common controls
D. all of the above
Answer: (SHOW ANSWER)

NEW QUESTION: 151
When determining the applicability of a specific security control, the security professional should utilize which type of guidance?
Response:
A. Categorization guidance
B. Selection guidance
C. Remediation guidance
D. Scoping guidance
Answer: D (LEAVE A REPLY)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

Valid CGRC Dumps shared by Actual4test.com for Helping Passing CGRC Exam! Actual4test.com now offer the **newest CGRC exam dumps**, the Actual4test.com CGRC exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com CGRC dumps with Test Engine here: https://www.actual4test.com/CGRC_examcollection.html (**725** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)