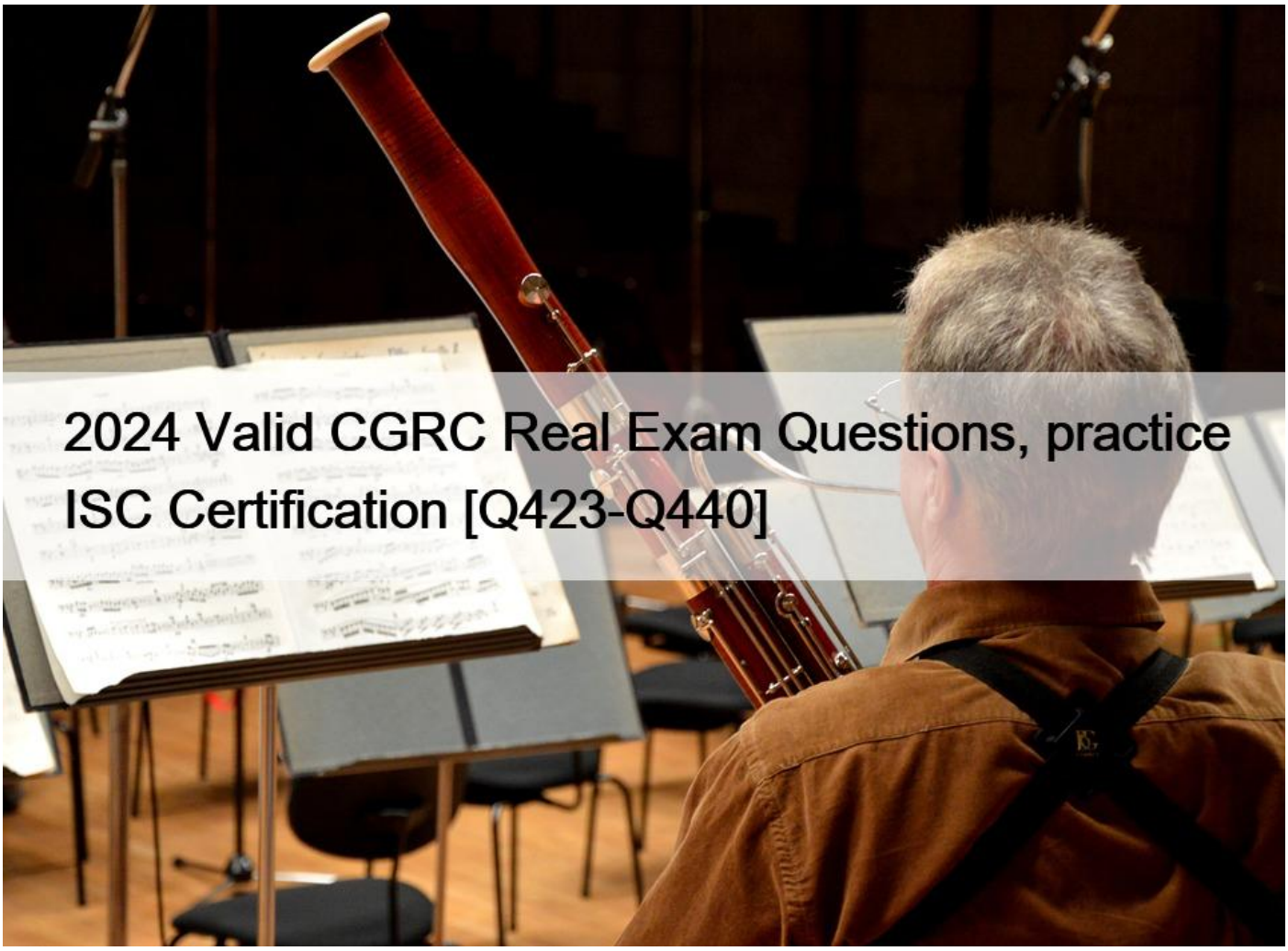
2024 Valid CGRC Real Exam Questions, practice ISC Certification [Q423-Q440



2024 Valid CGRC Real Exam Questions, practice ISC Certification Latest Success Metrics For Actual CGRC Exam (Updated 725 Questions) Q423. Who initiates system authorization process and has the full responsibility over the life cycle of an information system?

Response:
* Security Control Assessor (SCA) and Risk Executive
* Information System Owner (ISO)
* Authorizing Official (AO)
* Information System Security Officer (ISSO)

Q424. Which of the following is an Information Assurance (IA) model that protects and defends information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non- repudiation?

Response:
* Parkerian Hexad

* Capability Maturity Model (CMM)
* Classic information security model
* Five Pillars model

Q425. Which of the following is a subset discipline of Corporate Governance focused on information security systems and their performance and risk management?

Response:
* Lanham Act
* ISG
* Clinger-Cohen Act
* Computer Misuse Act

Q426. Who determines the required level of independence for security control assessors? Response:
* Information system owner (ISO)
* Information system security manager (ISSM)
* Authorizing official (AO)
* Information system security officer (ISSO)

Q427. Who is primarily responsible for categorizing the Information System? Response:
* IS program manager
* CIO
* Information system owner
* System architect

Q428. Fred is the project manager of the PKL project. He is working with his project team to complete the quantitative risk analysis process as a part of risk management planning. Fred understands that once the quantitative risk analysis process is complete, the process will need to be completed again in at least two other times in the project.

When will the quantitative risk analysis process need to be repeated? Response:
* Quantitative risk analysis process will be completed again after the plan risk response planning and as part of procurement.
* Quantitative risk analysis process will be completed again after the cost management planning and as a part of monitoring and controlling.
* Quantitative risk analysis process will be completed again after new risks are identified and as part of monitoring and controlling.
* Quantitative risk analysis process will be completed again after the risk response planning and as a part of monitoring and controlling.

Q429. _____ of Effort will drive size of testing team, rigor of testing, & amount of documentation required.

Response:
* Level
* Antecedent
* Worst
* Side

Q430. The Security Content Automation Protocol (SCAP) is a method for which of the following?

Response:
* Using specific standards to enable automated policy compliance evaluation
* Automating the documentation of security controls

* Facilitating interconnected systems to communicate regarding security control effectiveness
* Automating the review of the security plan (SP)

Q431. Which of the following statements about the authentication concept of information security management is true?

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

Q432. A system or system element that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application or required controls of the assessment of control effectiveness best defines:

Response:
* A high-Impact System
* An external system (or component)
* A major application
* A minor application

Q433. According to NIST SP 800-37 Rev 2, which role has a primary responsibility to report the security status of the information system to the authorizing official (OA) and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy?

Response:
* Information system security officer
* Independent assessor
* Common control provider
* Senior information assurance officer

Q434. Who is the official with the authority to formally assume responsibility for operating an IS at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Response:
* Authorizing Official (AO)
* Information Security Architect (ISA)
* Information System Owner (ISO)
* Chief Information Officer (CIO)

Q435. Risk acceptance when the external subsystem owner or service provider cannot fully meet security expectations should be based on the implementation of……..

Response:
* compensating controls. Otherwise, the organization may have to accept a greater degree of risk or determine that the risk is too great to accept and decline use of the external service or subsystem.

Guidance on
* compensating controls. Otherwise, the unorganization may have to accept a greater degree of risk or determine that the risk is too

great to accept and decline use of the external service or subsystem.

Guidance on
* compensating controls. Otherwise, the organization may have to reject a greater degree of risk or determine that the risk is too great to accept and decline use of the external service or subsystem.

Guidance on
* compensating controls. Otherwise, the organization may have to accept a greater degree of risk or determine that the risk is too great to reject and decline, use of the external service or system.

Guidance on

Q436. Which of the following statements about the availability concept of Information security management is true?

Response:
* It ensures that modifications are not made to data by unauthorized personnel or processes .
* It ensures reliable and timely access to resources.
* It determines actions and behaviors of a single individual within a system.
* It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

Q437. 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:
* Federal Enterprise Architecture
* Net-Centric Architecture
* Industry Standard Architecture
* Enterprise Architecture

Q438. 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:
* Common Controls
* Management controls
* Failed controls
* Alternative controls

Q439. What is not a responsibility of the Risk Executive (Function) in an organization’s ISCM?

Response:
* Participate in the configuration management process
* Review status reports from the ISCM process as input to information security risk posture and risk tolerance
* Oversee the organization’s ISCM program
* Provide input to mission/business process and information tier entities on ISCM strategy

Q440. 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:
* Segregation of duties
* Separation of duties

* Need to Know
* Due care

Genuine CGRC Exam Dumps Free Demo Valid QA's: https://www.braindumpsit.com/CGRC_real-exam.html]