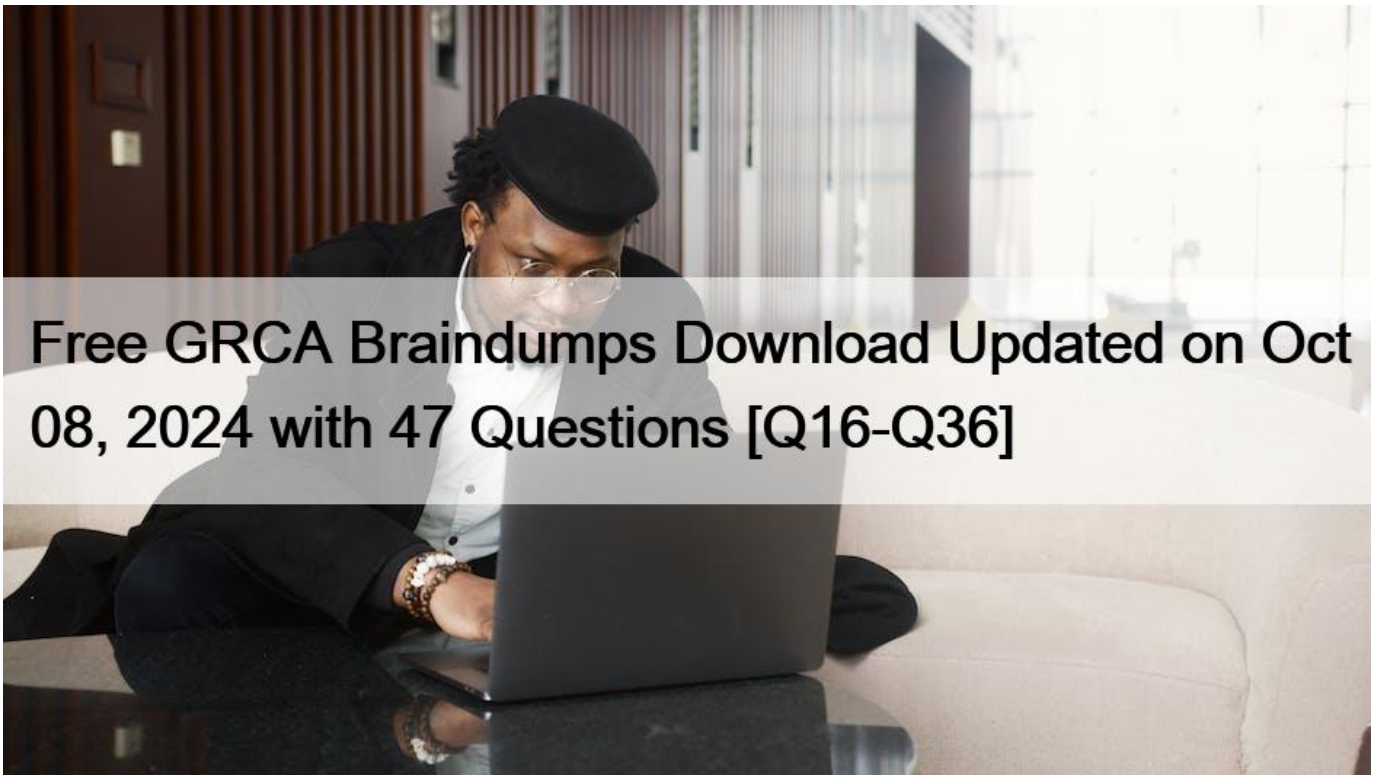
Free GRCA Braindumps Download Updated on Oct 08, 2024 with 47 Questions [Q16-Q36



Free GRCA Braindumps Download Updated on Oct 08, 2024 with 47 Questions
OCEG GRCA Exam Practice Test Questions

QUESTION 16

Which of the following is defined as “a measure of the desirable effect of uncertainty on objectives?
* Risk
* Compliance
* Reward
Risk is defined as a measure of the desirable effect of uncertainty on objectives. According to the ISO 31000 standard, risk is “the effect of uncertainty on objectives” which can be either positive (opportunity) or negative (threat). This definition encompasses the uncertainty that can impact the achievement of goals and objectives.

It highlights that risk is not just about potential losses but also about potential gains that come from taking risks.References:

* ISO 31000:2018 – Risk management – Guidelines

* NIST SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments

QUESTION 17

Which of these is defined as “internally directing, controlling and evaluating an entity, process or resource”
* Management
* Governance
* Assurance
Management is defined as “internally directing, controlling and evaluating an entity, process or resource.”
Management involves overseeing the day-to-day operations of an organization, making decisions, setting policies, and ensuring that the organization’s resources are used effectively to achieve its goals. This function includes planning, organizing, leading, and controlling organizational activities to meet established objectives.

References:

* ISO 9001:2015 – Quality management systems – Requirements

* COSO Internal Control – Integrated Framework

QUESTION 18

All Review Procedures in the GRC Assessment Tools must be followed to assess a particular element
* True. Thinking has been done for you.
* False. Use your professional judgement.
It is important to use professional judgment when conducting a GRC assessment, rather than rigidly following all review procedures in the GRC Assessment Tools. While these tools provide valuable guidelines and frameworks, each organization and situation is unique. Professional judgment allows for flexibility and adaptation of the procedures to fit the specific context andnuances of the assessment, ensuring more relevant and effective outcomes.References:

* ISO 19011:2018 – Guidelines for auditing management systems

* IIA Standards for the Professional Practice of Internal Auditing

QUESTION 19

Which of these is defined as “externally directing, controlling and evaluating an entity, process or resource”
* Assurance
* Management
* Governance

QUESTION 20

Follow-up on the implementation status of the recommendation based on high priority, due or overdue items or time-sensitive items is known as:
* Follow-Up by Process Owner
* Follow-Up by Independent Assurance
* Follow-Up by Targeted Review
Follow-up on the implementation status of recommendations based on high priority, due or overdue items, or time-sensitive items is known as Follow-Up by Targeted Review. This approach focuses on areas that are of critical importance or where timely implementation is essential. It helps ensure that the most significant risks are addressed promptly and that any delays in addressing recommendations are identified and managed.

References:

* IIA Standards for the Professional Practice of Internal Auditing

* COSO Internal Control – Integrated Framework

QUESTION 21

To evaluate operating effectiveness
* Conduct control testing
* Conduct substantive testing
To evaluate the operating effectiveness of controls, conducting control testing is essential. Control testing involves examining whether controls are operating as intended and are effective in mitigating risks. This type of testing assesses the design and implementation of controls to ensure they are functioning properly and achieving their intended purpose. Substantive testing, on the other hand, focuses on verifying the accuracy and validity of transactions and data, rather than the effectiveness of controls.References:

* COSO Internal Control – Integrated Framework

* ISO 31000:2018 – Risk management – Guidelines

QUESTION 22

Identifying root causes helps to
* Be more specific regarding who is to blame
* Find a solution to fixing not only this problem but potential other problems that result from the same root cause
Identifying root causes helps to find solutions that fix not only the current problem but also prevent other potential problems that stem from the same root cause. This approach leads to more sustainable and effective improvements by addressing the underlying issues rather than just the symptoms. It enhances the overall quality and reliability of processes and controls within the organization.References:

* ISO 31000:2018 – Risk management – Guidelines

* Root Cause Analysis: Improving Performance for Bottom-Line Results by Robert J. Latino, Kenneth C.

Latino, and Mark A. Latino

QUESTION 23

The parameters of an Assessment include
* Evidence, Tests and Outcomes
* Scope, Tests and Evidence
* Scope, Criteria and Nature of Testing
The parameters of an assessment include Scope, Criteria, and Nature of Testing. These elements define the boundaries and focus of the assessment:

* Scope:Defines the areas, processes, and activities to be assessed.

* Criteria:Specifies the standards, policies, and regulations against which the assessment will be conducted.

* Nature of Testing:Describes the types and extent of testing procedures that will be employed to gather evidence and evaluate compliance and performance.

These parameters ensure that the assessment is well-structured, targeted, and aligned with the objectives and requirements of the organization.References:

* ISO 19011:2018 – Guidelines for auditing management systems

* COSO Internal Control – Integrated Framework

QUESTION 24

When inspecting information, the Content Criteria provides a guide to evaluating which of these
* Design of the control
* Substance of the operation in the field
When inspecting information, the Content Criteria provides a guide to evaluating the design of the control.

Content Criteria help ensure that the controls are appropriately designed to achieve their intended purpose.

Evaluating the design involves assessing whether the control’s structure, procedures, and policies are adequate to mitigate identified risks and meet regulatory and organizational requirements.References:

* ISO 19011:2018 – Guidelines for auditing management systems

* COSO Internal Control – Integrated Framework

QUESTION 25

Producing Value and Protecting Value are trade-offs. You CANNOT do both at the same time. *
* True
* False
The statement that producing value and protecting value are trade-offs and cannot be done at the same time is false. In fact, both can and should be pursued concurrently. Effective governance, risk management, and compliance (GRC) strategies integrate the production of value (achieving business objectives and growth) with the protection of value (safeguarding assets, ensuring compliance, and managing risks). This integrated approach ensures sustainable performance and long-term success. Organizations that balance both aspects can achieve principled performance by reliably achieving objectives, addressing uncertainty, and acting with integrity.References:

* ISO 31000:2018 – Risk management – Guidelines

* COSO Enterprise Risk Management – Integrating with Strategy and Performance

QUESTION 26

A NEGATIVE assurance opinion or statement is
* An affirmative statement that subject matter conforms to the suitable criteria and is free from meaningful misunderstanding
* A statement that the assessment didn’t observe anything that makes us doubt whether subject matter conforms to the suitable criteria and is free from meaningful misunderstanding.
* A statement that the assessment encountered some limitations in what can be concluded and outside of those limitations a positive or negative statement can be offered.
A NEGATIVE assurance opinion or statement indicates that, based on the procedures performed and evidence obtained, the assurance provider did not identify any reasons to believe that the subject matter does not conform to the applicable criteria. This

form of opinion does not provide absolute assurance but rather limited assurance, suggesting that nothing came to the auditor’s attention that causes them to believe the subject matter is not fairly stated.References:

* AICPA Auditing Standards

* IIA Standards for the Professional Practice of Internal Auditing

QUESTION 27

What level of assurance is required for an assessment?
* Medium
* High
* Low
* An assessment may target any level of assurance. The key is to define this level prior to setting the purpose and parameters.

The level of assurance required for an assessment can vary depending on the purpose, scope, and objectives of the assessment. It is crucial to define the desired level of assurance (low, medium, or high) before beginning the assessment to ensure that the approach, methodology, and resources allocated are appropriate. This helps in setting clear expectations and aligning the assessment process with the organization’s risk tolerance and regulatory requirements.References:

* ISO 19011:2018 – Guidelines for auditing management systems

* COSO Enterprise Risk Management – Integrating with Strategy and Performance

QUESTION 28

How would the following test be classified?

The Assurance Provider inspects a RACI matrix for inclusion of best practice content.
* Control test
* Substantive test

Inspecting a RACI (Responsible, Accountable, Consulted, Informed) matrix for inclusion of best practice content is classified as a control test. This test evaluates whether the RACI matrix, a control tool, is designed and implemented according to best practices. It assesses the completeness and appropriateness of the matrix in defining roles and responsibilities, which is an aspect of control effectiveness.

References:

COSO Internal Control – Integrated Framework

ISO 31000:2018 – Risk management – Guidelines

QUESTION 29

Which of these is defined as “externally directing, controlling and evaluating an entity, process or resource”
* Governance
* Assurance
* Management

Governance is defined as “externally directing, controlling and evaluating an entity, process, or resource”. It involves establishing policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It ensures that the entity is operating effectively and in alignment with its objectives and regulatory requirements.

Governance encompasses a wide range of activities, including strategic planning, decision-making, and oversight, all aimed at achieving the entity’s goals while managing risk and ensuring compliance.References:

* ISO 38500:2015 – Information technology – Governance of IT for the organization

* OECD Principles of Corporate Governance

QUESTION 30

When planning an Assessment, it is important to
* INCLUDE the personnel who perform the work being assessed. They will help to inform Assessment staff and help to adjust parameters if necessary.
* NOT include the personnel who perform the work being assessed. They will pollute the process.
Including the personnel who perform the work being assessed in the planning process is important because they possess valuable insights and knowledge about the processes and controls in place. Their involvement helps to ensure that the assessment is accurately scoped and relevant parameters are set. They can provide context and clarify operational details, contributing to a more effective and targeted assessment. Moreover, their engagement can foster a cooperativeenvironment and facilitate smoother assessment execution.

References:

* ISO 19011:2018 – Guidelines for auditing management systems

* COSO Internal Control – Integrated Framework

QUESTION 31

What are the dimensions of TOTAL Performance?
* Effectiveness, Efficiency and Reponsiveness
* Agility, Efficiency and Effectiveness
* Effectiveness, Resiliency, and Agility
The dimensions of TOTAL Performance are Effectiveness, Resiliency, and Agility. Effectiveness refers to achieving the desired outcomes. Resiliency is the ability to recover from setbacks and continue operations.

Agility is the capacity to adapt quickly to changes and new opportunities. These three dimensions collectively ensure that an organization can perform well under various conditions and sustain its success over time.

References:

* ISO 9001:2015 – Quality management systems – Requirements

* COSO Enterprise Risk Management – Integrating with Strategy and Performance

QUESTION 32

Which one of these is most associated with a “measure of how well we are meeting obligations”
* Performance
* Risk
* Compliance
Compliance is most associated with a “measure of how well we are meeting obligations.” Compliance involves

adhering to laws, regulations, policies, and standards that apply to an organization. It ensures that the organization is fulfilling its legal, regulatory, and ethical obligations, thereby avoiding penalties, legal issues, and reputational damage. Compliance programs include policies, procedures, training, monitoring, and audits to ensure that all obligations are consistently met.References:

* ISO 19600:2014 – Compliance management systems – Guidelines

* NIST SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and Organizations

QUESTION 33

If (Inherent Risk x Control Risk) is low
* We should perform extra testing
* We may consider performing less testing
If the inherent risk and control risk are both low, we may consider performing less testing. Inherent risk refers to the risk of an event occurring without considering any controls, while control risk is the risk that controls will not prevent or detect the event. When both risks are low, it indicates that the likelihood of issues occurring and not being detected is minimal, allowing for a reduced level of testing. This approach helps in efficiently allocating resources while maintaining a reasonable level of assurance.References:

* AICPA Auditing Standards

* ISO 31000:2018 – Risk management – Guidelines

QUESTION 34

The key steps in the Assessment Process are
* Select, Assess, Monitor and Improve
* Plan, Perform, Report and Follow-Up
The key steps in the Assessment Process are Plan, Perform, Report, and Follow-Up. These steps provide a structured approach to conducting assessments, ensuring thorough evaluation and continuous improvement:

* Plan:Define the scope, objectives, and methodology.

* Perform:Execute the assessment according to the plan.

* Report:Document findings and provide recommendations.

* Follow-Up:Monitor the implementation of recommendations and improvements.

These steps help ensure assessments are systematic, objective, and effective in identifying areas for improvement.References:

* ISO 19011:2018 – Guidelines for auditing management systems

* COSO Internal Control – Integrated Framework

Updated Verified GRCA dumps Q&As - Pass Guarantee or Full Refund:
https://www.examcollectionpass.com/OCEG/GRCA-practice-exam-dumps.html]