PassQueen
a.k.a dumpsqueen.com

GRC Auditor Certification Exam

OCEG GRCA

Version Demo

Total Demo Questions: 6

Total Premium Questions: 66

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

An Assurance Provider observes one instance in which a control operator correctly performed a daily reconciliation. The control is intended to operate every business day throughout the year. What is the BEST conclusion from this observation alone?

A. The control is operating effectively because it was observed working.

B. The control design is ineffective because observation is not documentary evidence.

C. The observation supports implementation evidence but not a conclusion on operation throughout the period.

D. No further testing is needed unless an exception is reported by management.

ANSWER: C

Explanation:

The observation provides some evidence that the control was performed correctly on the day observed, but it is not sufficient to conclude that the control operated effectively throughout the year. Operating effectiveness requires evidence about consistent performance over the relevant period, including the required frequency and handling of exceptions. The Assurance Provider should design additional procedures that are proportionate to the assessment purpose and risk.

QUESTION NO: 2

Which of these is defined as "internally directing, controlling and evaluating an entity, process or resource"

A. Management

B. Governance

C. Assurance

ANSWER: A

Explanation:

Management is correct because OCEG distinguishes management as the internal activity of directing, controlling, and evaluating an entity, process, or resource. It is the operational function through which authorized leaders and managers organize work, allocate and oversee resources, make and implement decisions, monitor performance, and take action to keep activities aligned with objectives. In a GRC context, management turns governance direction into practical execution: it operates processes, maintains controls, responds to issues, and evaluates whether resources and activities are producing the intended results. The word “internally” is important because the definition concerns the ongoing administration and oversight of the organization’s own operations, rather than an independent review function. Management therefore provides the day-to-day direction and control needed for the organization to achieve objectives while addressing risk and meeting obligations. This terminology is consistent with OCEG’s integrated GRC model, which treats governance, management, and assurance as related but distinct roles in achieving reliable performance. See OCEG’s GRC Glossary and its overview of the GRC Capability Model (Red Book).

QUESTION NO: 3

In planning an Assessment, preliminary information indicates that a process has high inherent risk but mature controls that appear consistently applied. Which approach is MOST appropriate?

A. Perform no further work because mature controls eliminate inherent risk

B. Plan targeted control testing and adjust further testing only after evaluating the results

C. Perform only substantive testing because controls are irrelevant to inherent risk

D. Classify the process as low risk because the controls appear mature

ANSWER: B

Explanation:

High inherent risk means the process remains susceptible to significant problems before considering controls. The apparent maturity of controls may support testing their design and operating effectiveness, but it should not be accepted without evidence or automatically result in minimal work. The Assessment plan should use targeted control testing and determine whether substantive testing can be reduced only after the control evidence supports reliance.

QUESTION NO: 4

Which disciplines are integrated into GRC?

A. Audit and Assurance

B. Governance and Oversight

C. Strategy and Performance Management

D. Quality and Conformance

E. Information Privacy and Security

F. Compliance and Ethics

G. Risk and Decision Support

H. All of the above

ANSWER: H

Explanation:

All of the above is correct because GRC is an integrated approach, not a standalone department or a narrowly limited control activity. In practice, effective GRC connects audit and assurance, governance and oversight, strategy and performance management, quality and conformance, information privacy and security, compliance and ethics, and risk and decision support. These disciplines share information, objectives, controls, assessments, reporting, and accountability so that the organization can make informed decisions and achieve its objectives with integrity. For example, risk information should inform strategic choices and performance monitoring; governance establishes the direction and accountability for those choices; compliance, ethics, privacy, security, and quality requirements are incorporated into operations; and audit and assurance provide confidence that intended practices and controls are working. This coordinated model avoids disconnected or duplicative efforts and supports what OCEG calls Principled Performance: the reliable achievement of objectives while addressing uncertainty and acting with integrity. OCEG's GRC Capability Model describes the capabilities and relationships needed to establish this integrated system, rather than treating these areas as isolated functions. See OCEG: What Is GRC? and OCEG GRC Capability Model (Red Book).

QUESTION NO: 5

When writing a complete recommendation it is important to include

A. Recommendation with suggested or mandatory requirements to comply with to fix the problem

B. General comments about how to fix the problem

ANSWER: A

Explanation:

Recommendation with suggested or mandatory requirements to comply with to fix the problem is correct because an audit recommendation must translate an identified issue into a clear action that management can implement. A complete recommendation identifies the required or proposed corrective action and connects it directly to resolving the underlying problem, such as a control deficiency, process gap, or instance of noncompliance. This makes the recommendation useful as a management tool: the responsible party can understand what outcome is expected, determine an appropriate remediation plan, assign ownership, and track completion. Recommendations should be practical, sufficiently specific to support corrective action, and framed to promote compliance with applicable requirements or improvement of the control environment. Where an obligation is mandatory, the recommendation should make that necessity clear; where the auditor is offering a preferred improvement approach, it can appropriately be presented as a suggested action. This approach supports the purpose of audit reporting: communicating meaningful results that enable corrective action and continual improvement. OCEG's GRC approach emphasizes reliable achievement of objectives through effective governance, risk management, and compliance capabilities; actionable recommendations help organizations strengthen those capabilities. See OCEG's GRC Capability Model and ISO's overview of ISO 19011 auditing guidelines.

QUESTION NO: 6

Follow up should be restricted to the recommendations and action plan

A. True. Only follow-up on planned actions and controls.

B. False. Follow-Up should target the underlying risk. If the planned actions and controls are working, then the follow-up should identify and recommend changes.

C. False. Follow-up should target the underlying risk and determine whether actions and controls are effectively mitigating it; recommend changes if they are not.

ANSWER: C

Explanation:

False. Follow-up is a risk-focused activity, not merely a checklist confirming whether recommendations or action-plan tasks were completed. A sound follow-up process assesses whether implemented actions and controls have actually reduced, controlled, or otherwise treated the underlying risk to an acceptable level. This means evaluating the effectiveness of the response in practice, considering whether risk conditions, assumptions, or the control environment have changed, and determining whether further action is needed. Where actions do not mitigate the risk as intended, follow-up should result in appropriate revisions, additional treatment, escalation, or renewed assessment.

This approach aligns with OCEG's integrated GRC view: governance, strategy, performance, risk, compliance, culture, and conduct should be managed as interconnected elements rather than isolated activities. It also reflects ISO 31000's expectation that risk management be monitored and reviewed so that the effectiveness and suitability of risk treatments can be evaluated over time. See the OCEG GRC Capability Model and the ISO 31000:2018 Risk management—Guidelines.