DUMPSBOSS.

GRC Professional Certification Exam

OCEG GRCP

Version Demo

Total Demo Questions: 30

Total Premium Questions: 306

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

What practices are involved in analyzing and understanding an organization's ethical culture?

A. Developing a strategic plan to achieve the organization's long-term goals for improving ethical culture

B. Conducting a survey of employees every few years on their views about the organization's commitment to ethical conduct

C. Implementing a performance appraisal system to evaluate employee performance

D. Analyzing the climate and mindsets about how the workforce generally demonstrates integrity

ANSWER: D

Explanation:

Analyzing the climate and mindsets about how the workforce generally demonstrates integrity is correct because ethical culture is revealed by the shared expectations, assumptions, attitudes, and everyday behaviors that influence how people make and carry out decisions. Understanding that culture requires looking beyond formal policies to determine whether integrity is genuinely expected, supported, modeled by leaders, and applied when employees face pressure, uncertainty, or competing objectives.

Climate analysis examines the practical environment in which people work: the messages leaders reinforce, the extent to which people can raise concerns, how accountability is exercised, and whether decision processes align with stated values. Mindset analysis addresses how personnel actually perceive ethical responsibilities, including their willingness to speak up and their confidence that ethical conduct will be supported. Together, these perspectives provide evidence of whether integrity is embedded in the organization's operations rather than merely stated as an aspiration.

This approach aligns with OCEG's emphasis on an integrated, contextual understanding of organizational culture and conduct within GRC practice. OCEG describes its GRC Capability Model and related guidance at OCEG GRC Capability Model. Additional governance guidance on the importance of ethical culture is available in the OECD G20/OECD Principles of Corporate Governance.

QUESTION NO: 2

(How is the effect of uncertainty on objectives classified as either positive or negative?)

A. The positive effect of uncertainty is called reward, and the negative effect is called risk

B. The positive effect of uncertainty is called benefit, and the negative effect is called harm

C. The positive effect of uncertainty is called a benefit, and the negative effect is called a prospect

D. The positive effect of uncertainty is called prospect, and the negative effect is called obstacle

ANSWER: A

Explanation:

The positive effect of uncertainty is called reward, and the negative effect is called risk. This reflects the GRC view that uncertainty should be considered in relation to an organization's objectives rather than solely as a source of loss. When uncertainty creates the potential for achieving enhanced value, improved performance, or a favorable outcome beyond what was expected, it represents reward. When uncertainty creates the potential for an unfavorable impact on objectives, it represents risk. Treating these as the two directions of uncertainty supports balanced decision-making: organizations need to protect value while also recognizing and pursuing worthwhile value-creating possibilities. This approach is consistent with the broader risk-management principle that uncertainty can affect objectives in more than one direction. ISO 31000 defines risk as the effect of uncertainty on objectives and recognizes that an effect may be a positive or negative deviation from what is expected. OCEG's GRC framework likewise emphasizes principled performance, in which governance and management practices address both the protection and creation of value. See ISO 31000: Risk management—Guidelines and OCEG GRC Capability Model.

QUESTION NO: 3

What are the two aspects of value that Protectors are skilled at balancing within an organization?

A. Value creation and value protection

B. Value production and value preservation

C. Value measurement and value analysis

D. Value assessment and value reporting

ANSWER: A

Explanation:

Value creation and value protection is correct because OCEG describes effective GRC as an integrated capability that helps an organization reliably achieve objectives, address uncertainty, and act with integrity. In that context, Protectors contribute more than defensive oversight: they help the organization preserve the value it already has while enabling informed, responsible pursuit of new value. Value creation concerns achieving objectives, pursuing opportunities, improving performance, and supporting sustainable growth. Value protection concerns reducing avoidable loss and harm by managing risk, meeting obligations, safeguarding assets and reputation, and maintaining stakeholder confidence. These are complementary aspects of organizational value, not competing functions. A capable Protector balances them by applying governance, risk management, compliance, and assurance practices proportionately, so controls and risk decisions support the business rather than merely constrain it. This balance is central to OCEG's GRC approach and its Principled Performance concept, which connects principled conduct with reliable achievement of objectives. OCEG's overview of GRC and Principled Performance is available at OCEG: What Is GRC?. The broader GRC Capability Model resources can be accessed through OCEG's GRC Capability Model.

QUESTION NO: 4

What is the advantage of using technology-based inquiry for discovering events?

A. This inquiry prevents the need for employee surveys.

B. This inquiry eliminates the need to analyze information.

C. This inquiry focuses on unfavorable events.

D. This inquiry often provides information sooner than other methods.

ANSWER: D

Explanation:

"This inquiry often provides information sooner than other methods." is correct because technology-based inquiry can continuously collect, correlate, and analyze signals from operational systems, transactions, communications, monitoring tools, and other digital sources. This gives an organization the ability to identify an event or emerging issue close to the time it occurs, rather than waiting for a periodic review, a manually administered survey, or an individual to report it. Earlier information supports timely escalation, investigation, response, and corrective action—key capabilities for managing GRC-related events before their impacts increase. In OCEG's GRC approach, reliable and timely information helps decision-makers understand context, act with appropriate speed, and improve organizational performance. Technology does not merely gather data; its value in inquiry is its capacity to make relevant event information available rapidly and at scale, including through automated monitoring and alerts. This earlier visibility can strengthen resilience by allowing the organization to respond while there is still a meaningful opportunity to contain consequences and adapt operations. See OCEG's overview of integrated GRC at OCEG GRC Capability Model and its resource library at OCEG Resources.

QUESTION NO: 5

In the context of GRC, which is the best description of the role of assurance in an organization?

A. Allocating financial resources and evaluating their use to manage the organization's budget better.

B. Providing the governing body with opinions on how well its objectives are being met based on expertise and experience.

C. Designing and monitoring the organization's information technology systems to be accurate and reliable so management can be assured of meeting established objectives.

D. Objectively and competently evaluating subject matter to provide justified conclusions and confidence.

ANSWER: D

Explanation:

Objectively and competently evaluating subject matter to provide justified conclusions and confidence is the best description of assurance because assurance is an independent, evidence-based activity that enables stakeholders to place confidence in information, controls, processes, and the achievement of objectives. The evaluator considers defined subject matter against suitable criteria, gathers and assesses sufficient evidence, and communicates a conclusion that is supported by that evidence. Competence is essential: assurance conclusions must be formed by people with the knowledge, skills, and professional judgment needed to evaluate the matter reliably. Objectivity is equally important because the value of assurance depends on conclusions being free from undue bias or conflicts of interest.

Within a GRC program, assurance helps governing bodies and management understand whether governance, strategy, performance, risk management, compliance, and control activities are operating as intended. It does not merely report activity; it provides a defensible conclusion that supports informed oversight and decision-making. This role aligns with OCEG's emphasis on dependable information and effective oversight across the GRC capability model. See OCEG's GRC Capability Model and its GRCP certification overview for the integrated GRC concepts underlying assurance.

QUESTION NO: 6

(What is the definition of "Assurance"?)

A. Assurance is the practice of monitoring and controlling the organization's financial performance and reporting

B. Assurance is the establishment of policies and procedures to ensure compliance with applicable laws and regulations

C. Assurance is the act of objectively and competently evaluating subject matter to provide justified conclusions and confidence that statements and beliefs about the subject matter are true

D. Assurance is the process of identifying and mitigating risks that could negatively impact the organization's objectives

ANSWER: C

Explanation:

Assurance is correctly defined as the act of objectively and competently evaluating subject matter to provide justified conclusions and confidence that statements and beliefs about the subject matter are true. In the OCEG GRC framework, assurance is a distinct GRC capability that helps decision-makers place appropriate confidence in information, processes, controls, and outcomes. It requires a competent evaluation against suitable criteria, supported by sufficient and reliable evidence, so that the resulting conclusion is justified rather than merely an opinion or unsupported assertion.

The subject matter may include the design or operation of controls, compliance obligations, risk information, performance reporting, security practices, or the effectiveness of a governance, risk, and compliance program. The essential outcome is confidence: stakeholders can use the conclusion to make informed decisions and exercise oversight. The evaluation must be objective, meaning it is performed without inappropriate bias or conflicts that would undermine the credibility of the conclusion. This aligns with OCEG's treatment of assurance as a mechanism for obtaining reliable information about whether organizational objectives and related requirements are being met. See OCEG's GRC Capability Model (Red Book) and the IIA Global Internal Audit Standards for related assurance principles.

QUESTION NO: 7

(Why is independence considered important in the assurance process?)

A. It allows the assurance provider to make decisions without consulting the governing authority

B. It ensures that the assurance provider has no financial interest in the organization being evaluated

C. It guarantees that the assurance provider will not be influenced by external factors

D. It is a means to achieve objectivity and is important for enhancing the impartiality and credibility of the assurance process

ANSWER: D

Explanation:

“It is a means to achieve objectivity and is important for enhancing the impartiality and credibility of the assurance process” is correct because independence provides the conditions under which an assurance provider can form and communicate conclusions without inappropriate pressure, conflicts of interest, or responsibility for the activities being assessed. Objectivity is the resulting unbiased mental attitude; independence is a crucial structural and personal safeguard that supports it. When assurance personnel have appropriate standing, unrestricted access to relevant information, and the ability to report significant matters to the governing authority, stakeholders can place greater confidence in the work performed and the conclusions reached. This credibility is essential because assurance is intended to give decision-makers reliable insight into whether governance, strategy, performance, and compliance arrangements are achieving their objectives. OCEG’s GRC Capability Model describes assurance as an important component of an integrated approach to governing and managing the organization, supporting informed oversight and continual improvement. Independence therefore does not remove all possible influence, but it materially strengthens impartial judgment and trust in assurance results. See OCEG’s GRC Capability Model and its GRC guidelines and resources.

QUESTION NO: 8

What is the primary purpose of the ALIGN component in the GRC Capability Model?

A. To coordinate the monitoring and evaluation of the organization's governance, risk, and compliance activities.

B. To define the direction and objectives of an organization and design an integrated plan to address opportunities, obstacles, and obligations.

C. To establish communication channels and provide education to stakeholders about how the organization aligns its business operations to their needs.

D. To review and improve the organization’s policies and controls and ensure they are aligned to the operations of the business.

ANSWER: B

Explanation:

“To define the direction and objectives of an organization and design an integrated plan to address opportunities, obstacles, and obligations.” correctly describes the purpose of ALIGN in OCEG’s GRC Capability Model. ALIGN establishes the organizational context for GRC by connecting the organization’s mission, objectives, strategy, values, and stakeholder expectations to its approach for managing uncertainty and meeting requirements. This component is concerned with making deliberate choices about direction and priorities, then designing an integrated approach that helps the organization pursue opportunities, address obstacles that could affect objectives, and meet obligations such as legal, regulatory, contractual, and ethical commitments.

In practical terms, ALIGN ensures that GRC is not treated as a disconnected compliance exercise. Instead, it embeds principled performance into planning and decision-making so that governance, risk, and compliance activities support the organization’s intended outcomes. The integrated plan provides a foundation for subsequent operational activities, including establishing accountability, implementing controls, gathering information, and responding to issues. OCEG describes GRC as the integrated collection of capabilities that enables an organization to achieve objectives, address uncertainty, and act with integrity. See OCEG’s GRC Capability Model and its overview of GRC principles and concepts.

QUESTION NO: 9

What does agility in the context of the PERFORM component refer to?

A. The proficiency in building and maintaining relationships with partners and suppliers who must implement Perform actions and controls

B. The ability to quickly change direction in Perform actions and controls when things change

C. The capacity to innovate and develop new ways to implement Perform actions and controls

D. The capability to manage and resolve conflicts and disputes regarding Perform actions and controls

ANSWER: B

Explanation:

In OCEG's GRC Capability Model, PERFORM is concerned with taking actions and applying controls that address objectives, risks, requirements, and opportunities. Agility in this context is the organization's capacity to adjust those actions and controls promptly when conditions change. Changes may include emerging risks, altered priorities, new requirements, operational disruptions, or evidence that a current control approach is no longer producing the intended result. The ability to quickly change direction in Perform actions and controls when things change is therefore correct because it captures responsive execution rather than merely planning for change. Agility helps ensure that performance activities remain practical, proportionate, and aligned to objectives as the organization's internal and external environment evolves. It also supports resilient operations: responsible personnel can revise a control, reallocate resources, alter an implementation approach, or introduce an appropriate response without unnecessary delay while maintaining accountability. This interpretation is consistent with OCEG's integrated view of governance, risk management, and compliance, in which capabilities must work together dynamically to achieve reliable objectives. See OCEG's GRC Capability Model and its overview of the GRC Red Book.

QUESTION NO: 10

(Which of the following is the ultimate goal of Total Performance?)

A. To maximize profits and increase shareholder value

B. To achieve regulatory compliance and avoid penalties

C. To expand the organization's market share and customer base

D. A balance of effectiveness, efficiency, responsiveness, and resilience

ANSWER: D

Explanation:

The ultimate goal of Total Performance is **a balance of effectiveness, efficiency, responsiveness, and resilience**. In OCEG's integrated GRC approach, performance is not treated as a narrow financial or operational target. It is the organization's sustained ability to achieve its objectives dependably while operating in changing conditions and using resources appropriately. Effectiveness focuses on achieving intended objectives; efficiency concerns the appropriate use of time, money, people, and other resources; responsiveness enables the organization to recognize and adapt to changing circumstances; and resilience supports continued operation and recovery when disruptions occur. Together, these qualities describe performance that can endure rather than short-term results achieved at the expense of the organization's future capability. This balanced view fits OCEG's emphasis on integrated governance, risk management, and compliance as organizational capabilities that support reliable objective achievement, informed action under uncertainty, and integrity in conduct. Governance leaders therefore use objectives, risk information, controls, and assurance to maintain these dimensions in an appropriate balance as conditions evolve. OCEG describes its GRC Capability Model and the broader concept of Principled Performance at OCEG's GRC Capability Model and explains its integrated GRC perspective at What Is GRC?.

QUESTION NO: 11

Management receives a dashboard showing that all key risk indicators remain below their thresholds. However, an external change has made the underlying data source incomplete, and the dashboard has not been updated for two months. What should management do first?

A. Increase the thresholds so that the indicators remain within an acceptable range.

B. Validate the continued relevance, completeness, and timeliness of the indicators and their data.

C. Continue using the dashboard until an unfavorable event demonstrates that it is unreliable.

D. Eliminate all existing key risk indicators and measure only financial performance.

ANSWER: B

Explanation:

Management should determine whether the indicators and their data remain reliable and relevant before relying on the reported thresholds. Monitoring supports informed decisions only when information is sufficiently accurate, timely, and fit for the current context. A dashboard can create false confidence when its indicators no longer reflect changing conditions.

Raising thresholds would obscure rather than evaluate the effect of the change. Continuing to use the dashboard until an unfavorable event occurs is inconsistent with proactive review, and replacing all KRIs without analysis may discard useful measures that can be corrected or supplemented.

QUESTION NO: 12

At a very high level, how can an organization address an opportunity, obstacle, or obligation?

A. By avoiding any actions that could lead to uncertainty

B. By focusing on immediate goals and actions that don't present uncertainty

C. By obtaining risk insurance

D. By using design options such as Avoid, Accept, Share, and Control

ANSWER: D

Explanation:

By using design options such as Avoid, Accept, Share, and Control is correct because OCEG's GRC approach treats opportunities, obstacles, and obligations as matters that require deliberate action and design. At a high level, an organization selects an appropriate response strategy based on its objectives, context, risk appetite, available resources, and the nature of the issue. Avoiding changes the plan or activity so the matter is no longer encountered. Accepting recognizes and retains the matter within defined tolerances. Sharing allocates or distributes some effect, responsibility, or exposure through arrangements with other parties. Controlling establishes measures that influence causes, likelihood, impacts, conduct, or performance. These are broad design choices, not mutually exclusive operational steps; in practice, an organization may combine them and then implement supporting controls, accountability, monitoring, and assurance. This framing is consistent with OCEG's integrated view of governance, risk management, and compliance, which emphasizes reliably achieving objectives, addressing uncertainty, and acting with integrity. OCEG describes the GRC capability model and its principles at OCEG GRC Capability Model. The related risk-management principle of selecting and tailoring treatments to organizational context is also reflected in ISO 31000 risk management guidance.

QUESTION NO: 13

How do organizational values contribute to acting with integrity?

A. Adhering to established organizational values helps create a shared sense of purpose and direction, aligning actions and decisions with the organization's mission and goals

B. Organizational values contribute to acting with integrity by increasing the organizationâ€™s market share and profitability, which will satisfy shareholders to whom promises were made

C. Organizational values contribute to acting with integrity by allowing the organization to bypass certain legal and regulatory requirements

D. Organizational values contribute to acting with integrity by reducing the likelihood of enforcement actions because the organization is self-regulating

ANSWER: A

Explanation:

Adhering to established organizational values helps create a shared sense of purpose and direction, aligning actions and decisions with the organization's mission and goals. Integrity is not merely a personal characteristic; in an organizational context, it is reinforced when people have clearly communicated principles that guide how objectives should be pursued. Values such as honesty, accountability, fairness, respect, and transparency provide a practical decision-making compass, particularly when individuals face competing priorities, uncertainty, or pressure to achieve results.

Within the OCEG GRC Capability Model, organizational culture and leadership are essential to reliably achieving objectives while addressing uncertainty and acting with integrity. Shared values help translate the organization’s commitment to principled performance into consistent behaviors, decisions, escalation practices, and accountability at every level. When values are embedded in governance, policies, communications, incentives, and daily work, personnel can connect their actions to the organization’s purpose rather than treating ethical conduct as separate from performance. This alignment also supports stakeholder trust because the organization’s stated commitments are reflected in how it operates. See the OCEG GRC Capability Model and OCEG’s GRC resources for further context on principled performance and integrity.

QUESTION NO: 14

Why is it important for an organization to sense and analyze changes in context within the LEARN component?

A. To evaluate the effectiveness of the organization’s risk management framework

B. To comply with legal and regulatory requirements related to governance and risk management

C. To ensure that the organization’s financial statements are accurate and up to date

D. To determine necessary changes to the organization and to understand which changes are significant and which are distractions

ANSWER: D

Explanation:

To determine necessary changes to the organization and to understand which changes are significant and which are distractions is correct because LEARN in OCEG’s GRC Capability Model supports continual improvement through awareness, assessment, and adaptation. An organization operates in a changing internal and external context: its objectives, stakeholders, culture, resources, technologies, markets, laws, and risk environment can all change. Sensing these developments and analyzing their relevance enables decision-makers to identify when changes to strategies, processes, controls, or resource allocations are needed to preserve and improve principled performance.

Just as importantly, effective analysis distinguishes meaningful signals from information that does not warrant organizational action. This avoids reactive, inefficient changes while ensuring that material developments receive appropriate attention. Context monitoring therefore provides the evidence needed to learn from experience and from changing conditions, make informed adjustments, and remain aligned with organizational objectives and obligations. OCEG describes its GRC Capability Model as an integrated approach for reliably achieving objectives, addressing uncertainty, and acting with integrity; continuous learning and adaptation are essential to that outcome. See OCEG’s GRC Capability Model and the ISO 31000 risk-management guidance overview, which emphasizes monitoring and review in response to changes in internal and external context.

QUESTION NO: 15

How do values influence the way an organization operates?

A. They establish the organization’s code of conduct

B. They set voluntary boundaries for how the organization operates and often explain design decisions about the operating model

C. They dictate the organization’s pricing strategy and revenue generation

D. They determine the organization ' s market share and competitive positioning as part of assessing its financial value to shareholders

ANSWER: B

Explanation:

They set voluntary boundaries for how the organization operates and often explain design decisions about the operating model. In OCEG’s GRC Capability Model, values are the principles an organization chooses to uphold, which can impose commitments and limits beyond mandatory legal, regulatory, and contractual requirements. They therefore shape the organization’s appetite for particular actions and the manner in which it pursues objectives. Values are not merely aspirational statements: when embedded in governance, they inform choices about structures, authority, policies, processes, controls, incentives, resource allocation, and stakeholder relationships. For example, an organization that values privacy, safety, sustainability, or fairness may deliberately design its products and operating practices to meet higher internal standards than external rules require. These choices reflect how the organization intends to create and preserve value while acting consistently with its stated principles. This direct influence on permissible conduct and operating-model design is why values are a foundational element of principled performance. OCEG describes principled performance as reliably achieving objectives while addressing uncertainty and acting with integrity, which requires governance and management practices to be aligned with organizational values. See OCEG’s overview of the GRC Capability Model and its explanation of Principled Performance.

QUESTION NO: 16

How does Benchmarking contribute to the improvement of a capability?

A. By identifying potential legal and regulatory issues.

B. By comparing the capability ' s performance to industry standards or best practices.

C. By assessing the impact of organizational culture.

D. By evaluating the effectiveness of risk management campaigns.

ANSWER: B

Explanation:

Benchmarking improves a capability by comparing the capability’s current performance, practices, maturity, or outcomes with relevant external points of reference, such as recognized industry standards, peer organizations, or leading practices. This comparison provides meaningful context for evaluating whether current performance is adequate and identifies gaps between the organization’s present state and an attainable target state. The resulting insights can be used to prioritize improvement actions, establish realistic performance objectives, and adopt proven approaches that strengthen the capability over time.

In the OCEG GRC Capability Model, capabilities are managed and improved through disciplined evaluation, measurement, and adaptation. Benchmarking is valuable because it turns performance information into a comparative assessment rather than considering internal results in isolation. It supports informed decisions about where resources and attention will produce the greatest improvement in effectiveness, efficiency, and reliability. The correct answer is therefore *By comparing the capability ' s performance to industry standards or best practices.* See OCEG’s overview of its GRC Capability Model and its GRC resources for the broader performance and improvement context.

QUESTION NO: 17

What is the role of key risk indicators (KRIs)?

A. KRIs are subjective measures that are not based on any specific risk assessments or data so they only provide a high-level assessment of threats

B. KRIs are indicators that help govern, manage, and provide assurance about risk related to an objective

C. KRIs are used to evaluate the performance of the risk management and compliance departments

D. KRIs are only relevant for governmental entities and have no role in commercial enterprises

ANSWER: B

Explanation:

KRIs are indicators that help govern, manage, and provide assurance about risk related to an objective. In the OCEG GRC Capability Model, risk is understood in relation to objectives: it is the effect of uncertainty on objectives. KRIs provide measurable, timely information about changes in risk exposure, risk drivers, or conditions that may affect the achievement of those objectives. By establishing thresholds and monitoring trends, an organization can recognize increasing exposure early, escalate matters to the appropriate decision-makers, and take action before risk events materially disrupt performance or compliance. This makes KRIs useful across all three GRC components: they inform governance oversight and decisions, support management actions and resource allocation, and supply evidence that risk is being monitored for assurance purposes. Effective KRIs are selected because they are relevant to a defined objective and risk context, are supported by reliable data, and prompt a defined response when tolerance levels are approached or exceeded. They are therefore a practical mechanism for connecting risk intelligence to organizational performance and resilient achievement of objectives. OCEG discusses the objective-centered nature of GRC in its GRC Capability Model (Red Book); further practical context on risk indicators is available from the Institute of Risk Management.

QUESTION NO: 18

What is the purpose of implementing ongoing and periodic review activities?

A. To eliminate the need for external audits.

B. To reduce the overall cost of operations.

C. To gauge the effectiveness, efficiency, responsiveness, and resilience of actions and controls.

D. To have documentation for use in defending against enforcement or legal actions.

ANSWER: C

Explanation:

The purpose of ongoing and periodic review activities is **to gauge the effectiveness, efficiency, responsiveness, and resilience of actions and controls.** In OCEG's GRC approach, reviews provide timely information about whether an organization's responses and supporting controls are performing as intended and continue to support reliable achievement of objectives. This is more than a simple compliance check: it evaluates whether actions produce the desired results (effectiveness), use resources appropriately (efficiency), adapt appropriately as conditions, requirements, or incidents change (responsiveness), and can withstand or recover from disruption (resilience).

Ongoing review embeds monitoring into normal operations so that emerging issues, control failures, and changing risks can be identified promptly. Periodic reviews provide a more deliberate reassessment at defined intervals, helping decision-makers evaluate trends, validate continued suitability, and determine whether improvements are needed. Together, these activities create feedback that supports continual improvement of the GRC capability and strengthens confidence in organizational performance. OCEG describes GRC as an integrated capability for reliable achievement of objectives while addressing uncertainty and acting with integrity; reviewing actions and controls is essential to maintaining that reliability. See OCEG GRC Capability Model and guidelines and OCEG's GRC overview.

QUESTION NO: 19

In which organizational departments do Protectors typically advise and work?

A. Supply chain, logistics, and procurement

B. Research and development, engineering, and production

C. Board, strategy, risk, compliance, ethics, human resources, legal, security, quality, internal control, and audit

D. Sales, marketing, finance, and customer service

ANSWER: C

Explanation:

Board, strategy, risk, compliance, ethics, human resources, legal, security, quality, internal control, and audit is correct because OCEG uses “Protectors” to describe professionals whose work helps the organization address uncertainty, act with integrity, and safeguard its people, assets, operations, and objectives. Their responsibilities are inherently cross-functional: they may provide governance and risk insight to the board and strategy functions; establish or oversee compliance, ethics, legal, security, quality, and internal-control practices; and work with human-resources and audit teams to promote accountable conduct and assurance. Protectors are therefore not defined by a single operational department. Rather, they commonly serve in specialist oversight and assurance disciplines while advising leaders and business functions throughout the organization. This broad placement reflects OCEG’s integrated GRC approach, in which governance, strategy, performance, risk, compliance, culture, and assurance must be coordinated instead of managed as disconnected silos. OCEG’s GRC Capability Model describes this integrated view of organizational capabilities and the roles that support reliable achievement of objectives. See the OCEG GRC Capability Model and OCEG’s overview of what GRC is.

QUESTION NO: 20

What is the role of sensemaking in understanding the internal context?

A. Sensemaking involves analyzing the organization’s supply chain to identify potential bottlenecks and make any necessary changes in how it is managed.

B. Sensemaking involves evaluating the organization’s sense of all aspects of its culture so that improvements can be made.

C. Sensemaking involves conducting financial audits to make sense of the financial condition of the organization and ensure compliance with accounting standards.

D. Sensemaking involves continually watching for and making sense of changes in the internal context that have a direct, indirect, or cumulative effect on the organization.

ANSWER: D

Explanation:

Sensemaking involves continually watching for and making sense of changes in the internal context that have a direct, indirect, or cumulative effect on the organization. In the OCEG GRC Capability Model, understanding context is an ongoing activity rather than a one-time assessment. Internal context includes the organization’s purpose, strategy, governance structure, people, culture, capabilities, resources, processes, information, and relationships. Sensemaking enables decision-makers to notice meaningful changes across these interconnected elements, interpret what those changes mean, and determine their potential effect on objectives and performance.

This continuing interpretation is important because changes may not be significant in isolation but can become material when combined with other conditions or when they persist over time. For example, a change in organizational structure, workforce capabilities, leadership priorities, or technology may alter how reliably objectives can be achieved. By continually observing and interpreting these developments, the organization can keep its actions, controls, and decisions aligned with its actual operating environment. OCEG describes GRC as a capability for reliably achieving objectives while addressing uncertainty and acting with integrity; informed awareness of internal context supports each of those outcomes. See OCEG GRC Guidelines and OCEG’s GRC Capability Model.

QUESTION NO: 21

What is the purpose of conducting after-action reviews?

A. To determine if, when, how, and what to disclose regarding unfavorable events

B. To provide timely incentives to employees for favorable conduct

C. To uncover root causes of favorable and unfavorable events and improve proactive, detective, and responsive actions and controls

D. To establish a tiered approach for responding to unfavorable events

ANSWER: C

Explanation:

The purpose of an after-action review is to uncover root causes of favorable and unfavorable events and improve proactive, detective, and responsive actions and controls. In the OCEG GRC approach, learning from outcomes is an essential feedback mechanism: organizations examine what occurred, identify the conditions and decisions that contributed to the result, and use those insights to improve how objectives are achieved, risks are addressed, and misconduct or failures are handled. This review is not limited to incidents with harmful consequences. Reviewing successful outcomes is equally valuable because it identifies practices, controls, and enabling conditions that can be retained, repeated, or scaled.

A useful review produces practical lessons and feeds them back into the organization's governance, risk, compliance, and performance processes. Its outputs can include refinements to policies, procedures, ownership, monitoring, escalation, training, and response capabilities. In this way, the review supports continual improvement rather than merely documenting an event after it has concluded. OCEG describes GRC as an integrated capability for reliably achieving objectives while addressing uncertainty and acting with integrity; systematic learning from events helps strengthen that capability. See OCEG's GRC Capability Model and the NIST Cybersecurity Framework, which emphasizes learning from incident response activities to improve future practices.

QUESTION NO: 22

Which statement is FALSE?

A. The organization should have an education plan for each target population indicating what they should know about the GRC capability and their responsibilities for GRC activities.

B. Regardless of role, everyone in the organization should receive the same curriculum and the same education activities to ensure consistent understanding.

C. The organization should conduct a needs assessment to determine the training that will address high-risk situations and develop a training plan for each job or job family.

D. The organization should identify legally mandated education, including who must be educated, the content required, the time required, and methods that may be used for each required course.

ANSWER: B

Explanation:

"Regardless of role, everyone in the organization should receive the same curriculum and the same education activities to ensure consistent understanding" is the false statement. An effective GRC education program establishes a common baseline of awareness, but it must also be tailored to the responsibilities, decision authority, activities, and risk exposure of each target population. For example, governing bodies, senior management, risk owners, control operators, compliance personnel, and general employees each need education that enables them to fulfill their particular responsibilities within the organization's GRC capability.

Providing identical education to every person can leave important role-specific knowledge unaddressed. It may also devote resources to content that is not relevant to particular jobs. A needs-based approach helps the organization determine the appropriate depth, content, delivery method, and frequency of education for job roles or job families, including training

needed to meet regulatory or legal obligations. This approach supports OCEG's emphasis on aligning GRC practices with organizational objectives, culture, and the actual responsibilities assigned to people. See OCEG's overview of GRC Capability Model (GRC Red Book) and its GRC resources.

QUESTION NO: 23

What is the role of assurance actions and controls in the IACM?

A. They are focused on identifying and punishing non-compliant behavior within the organization

B. They are used to evaluate the management and governance controls with regard to achieving financial objectives

C. They provide additional information beyond management and governance actions and controls to evaluate subject matter

D. They are limited to financial audits and do not address other aspects of performance, risk, and compliance

ANSWER: C

Explanation:

They provide additional information beyond management and governance actions and controls to evaluate subject matter. In OCEG's Integrated Assurance, Control, and Management (IACM) approach, assurance is a distinct source of objective insight about whether the organization's GRC-related activities, controls, and outcomes are adequate and effective. Assurance activities gather, assess, validate, and communicate information so that decision-makers can evaluate relevant subject matter with an appropriate level of confidence. This information supplements the information generated through normal management activity and governance oversight; it is not confined to a particular discipline such as finance. The assurance role can be performed through mechanisms such as internal audit, independent reviews, testing, monitoring, assessments, and other evaluation activities, depending on the organization's needs and the nature of the subject being evaluated. By creating reliable information and reporting it to the appropriate stakeholders, assurance supports informed decisions, accountability, and continual improvement across performance, risk, and compliance objectives. OCEG describes assurance as an essential component of an integrated GRC capability and distinguishes it from the activities used to direct, manage, and control the organization. See OCEG GRC guidelines and resources and OCEG's GRC capability information.

QUESTION NO: 24

In the IACM, what is the role of Compound/Accelerate Actions & Controls?

A. To identify and address any potential conflicts of interest that may compound or accelerate enforcement actions against the company.

B. To enhance the brand image and reputation of the organization.

C. To accelerate and compound the impact of favorable events to increase benefits and promote the future occurrence.

D. To accelerate and compound the benefits of reducing costs.

ANSWER: C

Explanation:

"To accelerate and compound the impact of favorable events to increase benefits and promote the future occurrence" correctly describes the Compound/Accelerate category in OCEG's Integrated Actions and Controls Model (IACM). The IACM recognizes that governance, risk, and compliance activities are not limited to avoiding or reducing adverse outcomes. Organizations should also deliberately respond to favorable events, conditions, and results in ways that increase the value obtained from them and make similar positive outcomes more likely in the future.

Compound/Accelerate Actions & Controls therefore support the organization in building on success. For example, when a control improvement, business initiative, customer response, or operational practice produces a beneficial result, the organization may scale it, reinforce the enabling conditions, apply the learning elsewhere, or invest additional resources to increase its impact. The emphasis is on amplifying beneficial effects and encouraging recurrence, rather than merely

recognizing a positive outcome. This approach reflects OCEG's broader view that effective GRC helps organizations reliably achieve objectives, address uncertainty, and act with integrity. See OCEG's overview of the GRC Capability Model and its OCEG resource library and GRC guidance.

QUESTION NO: 25

An organization maintains a register of legal, regulatory, contractual, and voluntary obligations. A review finds that the register identifies each obligation and its source, but it does not identify the business activities, actions, controls, or evidence used to address them. Which capability weakness is most significant?

A. The register does not establish traceability from obligations to actions, controls, and evidence of effectiveness.

B. The register does not classify all obligations as either mandatory or voluntary.

C. The register does not require the compliance function to operate every related control.

D. The register does not include a separate entry for every possible unfavorable event.

ANSWER: A

Explanation:

The most significant weakness is the absence of traceability from obligations to the actions, controls, and evidence that demonstrate they are addressed. Identifying obligations is necessary, but compliance requires the organization to determine how each applicable obligation is implemented in practice and how effectiveness can be evidenced.

Simply increasing the number of obligations in the register or assigning every obligation to the compliance function would not establish accountable implementation. A mapped relationship supports ownership, monitoring, assurance, and timely response when an obligation or operating condition changes.

QUESTION NO: 26

What are some examples of environmental factors that may influence an organization ' s external context?

A. Climate and natural resources

B. Organizational procurement, vendor selection, and contract negotiation for hazardous waste disposal

C. Organizational performance metrics, goal setting, and progress tracking regarding climate-related projects

D. Organizational response to new carbon emission regulations

ANSWER: A

Explanation:

Climate and natural resources are examples of environmental factors in an organization's external context because they arise outside the organization yet can materially affect its objectives, operations, risk profile, and ability to create value. Climate conditions can include changing weather patterns, extreme events, temperature changes, water stress, flooding, wildfire exposure, and longer-term physical effects associated with climate change. These conditions can disrupt facilities, personnel, logistics, supply chains, insurance availability, and business continuity planning. Natural resources are similarly external considerations: the availability, quality, location, and sustainability of water, energy, land, minerals, and other inputs may affect sourcing, production capacity, costs, and stakeholder expectations. A sound GRC approach identifies such contextual conditions, evaluates their potential impact on organizational objectives, and incorporates them into strategy, risk assessment, resilience, and decision-making. OCEG's GRC Capability Model emphasizes understanding context and managing uncertainty in pursuit of principled performance; environmental conditions are a meaningful source of that uncertainty. See the OCEG GRC Capability Model and ISO's overview of ISO 31000 risk management.

QUESTION NO: 27

How can "assurance competence" contribute to the level of assurance provided?

A. It is solely based on the assurance provider's credentials and ensures the highest level of assurance

B. It is determined by the number of years the assurance provider has been in the industry and ensures high levels of assurance

C. A greater degree of it allows the assurance provider to use sophisticated, professional, and structured techniques to evaluate the subject matter, resulting in a higher level of assurance

D. It is only relevant for external audits and does not apply to internal assurance activities and level of assurance

ANSWER: C

Explanation:

“A greater degree of it allows the assurance provider to use sophisticated, professional, and structured techniques to evaluate the subject matter, resulting in a higher level of assurance” is correct because assurance competence concerns the knowledge, skills, experience, professional judgment, and methodological capability needed to perform an assurance engagement effectively. Competent assurance providers can appropriately define scope, identify relevant criteria and risks, obtain and evaluate sufficient and reliable evidence, and apply disciplined procedures to reach well-supported conclusions. These capabilities directly affect the rigor and reliability of the work and therefore the level of assurance that can reasonably be provided. In OCEG’s GRC approach, assurance is not merely a matter of holding credentials or having time in the field; it is a structured activity that evaluates whether objectives are achieved, risks are managed, and controls operate as intended. The provider’s competence enables the use of suitable, systematic techniques and sound professional judgment throughout that evaluation. Greater competence supports a more robust assessment of the subject matter and more credible assurance for decision-makers. This principle applies across assurance contexts, including internal assurance functions, and aligns with the expectation that assurance work be performed by individuals with appropriate proficiency and due professional care. See OCEG’s GRC Capability Model and guidance resources and The Institute of Internal Auditors’ Global Internal Audit Standards.

QUESTION NO: 28

What type of activities are typically included in post-assessments?

A. Financial audits and budget reviews.

B. Employee performance evaluations and appraisals.

C. Market research and customer surveys.

D. Lessons learned, root-cause analysis, after-action reviews, and other evaluative activities.

ANSWER: D

Explanation:

Lessons learned, root-cause analysis, after-action reviews, and other evaluative activities are typically included in post-assessments because these activities examine what happened after an event, initiative, assessment, or response activity and turn that experience into actionable improvement. In the OCEG GRC Capability Model, assessment is not merely a point-in-time check; it supports learning, adaptation, and the continued improvement of the organization’s approach to governing, managing risk, and ensuring compliance. A post-assessment therefore collects relevant evidence about outcomes, identifies contributing conditions and underlying causes, documents observations, and determines improvements that should be incorporated into future planning and operations.

Lessons learned preserve useful knowledge for reuse. Root-cause analysis looks beyond immediate symptoms to determine the factors that produced an issue or result. After-action reviews provide a structured discussion of performance, outcomes, and opportunities to improve. Together, these evaluative practices enable informed corrective actions, strengthen capabilities over time, and help ensure that results from monitoring, audits, incidents, projects, or exercises are translated

into meaningful organizational learning. This aligns with OCEG's emphasis on reliable achievement of objectives through an integrated GRC approach. See the OCEG GRC Capability Model overview and OCEG's GRC resources.

QUESTION NO: 29

What should be avoided to maintain the integrity of the inquiry process?

A. Any inquiries that require identification of the respondent

B. Any automated analysis of information and findings

C. Any actual or perceived connection between inquiry responses and individual performance appraisals

D. Any use of technology-based inquiry methods

ANSWER: C

Explanation:

Any actual or perceived connection between inquiry responses and individual performance appraisals should be avoided because inquiry processes depend on participants providing candid, reliable information. When people believe that their answers could influence their personal evaluation, compensation, promotion prospects, or standing with managers, they may withhold concerns or tailor responses to what seems safest. This undermines the quality of the information collected and weakens confidence in the process, even where no direct link to appraisal decisions actually exists. Maintaining a clear separation between inquiry responses and individual performance management helps protect confidentiality, supports psychological safety, and encourages open reporting of issues, risks, and opportunities for improvement. OCEG's GRC approach emphasizes obtaining meaningful information and fostering a culture in which people can communicate concerns and insights without fear of adverse personal consequences. The inquiry owner should communicate the purpose of the inquiry, how responses will be handled, who can access them, and that responses will be used appropriately for organizational learning and improvement rather than individual appraisal. See OCEG's overview of the GRC Capability Model and its guidance on building a speak-up culture in the OCEG resource library.

QUESTION NO: 30

In the context of Total Performance, how is responsiveness measured in the assessment of an education program?

A. The number of new courses added to the education program each year.

B. The number of positive reviews received for the education program.

C. The percentage of employees who pass the final assessment.

D. Time taken to educate a department, time to achieve 100% coverage, and time to detect and correct errors.

ANSWER: D

Explanation:

Time taken to educate a department, time to achieve 100% coverage, and time to detect and correct errors is the correct measure because responsiveness evaluates the speed with which an education program can be deployed, completed across its intended audience, and adjusted when issues arise. In a Total Performance assessment, the organization needs evidence that its education capability can respond promptly to new requirements, changed risks, revised policies, or identified knowledge gaps. "Time to educate" indicates how rapidly relevant training can reach a defined group. The time to full coverage shows how quickly the program reaches the complete required population, rather than only its initial launch. The time to detect and correct errors assesses the program's ability to identify shortcomings in content, delivery, participation, or implementation and restore effective operation quickly. Together, these measures focus on operational agility and timely adaptation, which are central to responsiveness. They can be tracked consistently over time and used to establish targets for improving the education program's performance. This approach aligns with OCEG's emphasis on measuring GRC capability performance through practical, outcome-oriented measures that support reliable achievement of objectives. See the OCEG GRC Capability Model overview and OCEG's official resources.