

Q. 1 Which of the following is the "key" to corporate governance? *

- ☒ To support the board responsibilities only at senior management level
- ☐ To respect the duties and responsibilities of senior managers and let them manage the affairs of the entire business
- ☐ To tightly control the rights and responsibilities across the entire business
- ☐ To distribute rights and responsibilities across the entire business

Explanation:- As per page 6 of GRC compatibility Model version 3 - When responsibilities are spread out across a significant number of individuals, each must fully understand and appreciate the impact his or her actions and decisions have on other parts of the organization, and how others may affect them.

[Report Error](#)

Q. 2 In order to practice Principled Performance an organization must be concerned with the governance, management and assurance of: *

- ☐ Performance, Controls and Ethics
- ☐ Controls, Risk and Ethics
- ☒ Performance, Risk and Compliance

Explanation:- As per page 13 of GRC compatibility Model version 3 - the ALIGN component focuses to Align performance, risk and compliance objectives, strategies, decision-making criteria, actions and controls with the context, culture and stakeholder requirements.

- ☐ Governance, Risk and Compliance

[Report Error](#)

Q. 3 An integrated approach to GRC involves *

- ☒ Applying a common vocabulary, approach and technology infrastructure to GRC processes.

Explanation:- As per page 4 of GRC compatibility Model version 3 - Integrating GRC capabilities is having a unified vocabulary and taxonomies for information; establishing common repositories for data, documents, and information;

- ☐ Consolidation of governance, risk and compliance processes.

- ☐ Consolidation of the various risk silos.

- ☐ Consolidation of the technology infrastructure related to GRC processes.

Report Error

Q. 4 Governance can be performed by all of the following groups EXCEPT: *

- ☒ IT Steering Committee

- ☐ Board of Directors

- ☐ Project Committee

Explanation:- As per GRC compatibility Model version 3, the Principled Performance View of Integration looks at the governance, management, and assurance of performance, risk, and compliance. Each of these activities encompasses many individual roles and sets of responsibilities and lists the role of the Governing Authority, Chief Financial Officer and Managers, Risk Executive and Managers, Compliance and Ethics Executive and Managers, Chief Information Executive and Managers, Human Resources Executive and Managers, Internal Audit Executive and Managers and Business Unit Operator and Managers

- ☐ Audit Committee

Report Error

Q. 5 The three main roles in the organization that must work together to achieve Principle Performance are: *

☐ Senior Management, Line Management, and Auditors

☐ Governance, Senior Management, and Line Managers

☐ Board, Senior Management, and Line Managers

☒ Governance, Management, and Assurance

Explanation:- As per GRC compatibility Model version 3, the Principled Performance View of Integration looks at the governance, management, and assurance of performance, risk, and compliance

[Report Error](#)

Q. 6 Principled Performance requires adherence to all of the following EXCEPT: *

☐ Addressing uncertainty

☒ Ensuring compliance with all laws and regulations

Explanation:- As per GRC compatibility Model version 3, the forward-thinking organizations have adopted a vision of Principled Performance — a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity

☐ Acting with integrity

☒ Reliable achievement of objectives

[Report Error](#)

Q. 7 Which of the following is NOT an element of the OCEG GRC Capability Model version 3.0? *

☐ Governance

Explanation:- As per GRC compatibility Model version 3, Direction is element of align, Assurance is element of review and Education is element of perform

☐ Assurance

☐ Direction

☒ Education

[Report Error](#)

Q. 8 Many roles have a direct responsibility for GRC activities. Which of the following roles has a less direct responsibility for GRC activities than the others? *

☐ Chief Information Officer

☐ Chief Risk Officer

☐ Chief Sales Officer

Explanation:- As per GRC compatibility Model version 3, the Principled Performance View of Integration looks at the governance, management, and assurance of performance, risk, and compliance

☒ Chief Compliance Officer

[Report Error](#)

Q. 9 According to the Red Book, which of the following is a Universal Outcome of Principled Performance? *

☐ Develop Improvement Plan

☒ Improve Responsiveness and Efficiency

Explanation:- According to the Red Book, a Universal Outcome of Principled Performance is to Improve Responsiveness and Efficiency. This means that an organization that values principled performance is able to quickly respond to changes in the environment and operate more efficiently, while also adhering to ethical principles and compliance requirements. This outcome is a result of the organization's commitment to ethical and responsible behavior, which helps to build trust and confidence among stakeholders. By being responsive and efficient, the organization is better able to achieve its goals and fulfill its mission while also meeting the expectations of its stakeholders.

☐ Increase Corrective Controls

☒ Assess Value of the Organization

[Report Error](#)

Q. 10 The definition of Principled Performance is: *

- ☐ The consistent achievement of goals, while addressing risks, and acting ethically
- ☐ The reliable achievement of the organizations goals while acting responsibly
- ☒ The reliable achievement of objectives, while addressing uncertainty and acting with integrity

Explanation:- As per the OCEG GRC Capability Model (Red Book) The vision of Principled Performance — a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity

- ☒ The reliable achievement of reducing risks to an acceptable level with being in compliance with mandatory and voluntary boundaries

[Report Error](#)

Q. 11 The OCEG GRC Capability Model (Red Book) is composed of which of the following? *

- ☐ 8 Components and 33 Elements
- ☒ 4 Components and 20 Elements

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) The OCEG GRC Capability Model (Red Book) is composed of 4 Components and 20 Elements

- ☐ 10 Components and 30 Elements
- ☒ 5 Components and 25 Elements

[Report Error](#)

Q. 12 A threat is *

- ☐ An event or condition that has, on balance, an undesirable effect on achieving objectives

Explanation:- Option2: An event or condition that has, on balance, an undesirable effect on achieving objectives. Explanation: A threat is defined as an event or condition that has, on balance, an undesirable effect on achieving objectives. It refers to anything that can potentially harm or negatively impact an organization's operations, assets, or objectives. Option1 (A measure of likelihood that an adverse event will take place) is not the correct definition of a threat. While likelihood is a factor considered in assessing threats, it is not the definition itself. Option3 (A type of risk) is not an accurate definition of a threat. Threats are different from risks. Risks involve the likelihood of a threat occurring and the potential impact it may have. Option4 (Always an external force that can harm the organization) is not true. While threats can come from external sources, they can also originate internally within an organization. Examples include security breaches, internal fraud, or system failures. Therefore, the correct definition of a threat is Option2: An event or condition that has, on balance, an undesirable effect on achieving objectives.

- ☐ A measure of likelihood that an adverse event will take place

- ☐ Always an external force that can harm the organization

- ☒ A type of risk

Report Error

Q. 13 Which of the following is NOT one of the Universal Outcomes of Principled Performance? *

- ☐ Prevent, detect and reduce adversity and weaknesses

- ☐ Assess human capital efficiency

Explanation:- According to OCEG GRC Capability Model (Red Book) Assess human capital efficiency is not an Universal Outcomes of Principled Performance

- ☐ Stay ahead of the game

- ☒ Optimize economic value and values

Report Error

Q. 14 Which of the following is NOT a component of the OCEG GRC Capability Model version 3.0? *

☐ Learn

☐ Review

☐ Perform

☒ Proact

Explanation:- As per the OCEG GRC Capability Model (Red Book) Proact is not a component of the OCEG GRC Capability Model version 3.0 instead Align is.

[Report Error](#)

Q. 15 Governance is: *

☐ The systematic application of processes and structures that enable an organizations to identify and monitor risk.

☐ The culture, values, mission, structure and layers of policies, processes and measures by which organizations are directed and controlled.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) GRC is viewed as a well-coordinated and integrated collection of all of the capabilities necessary to support Principled Performance at every level of the organization

☐ Limited to the activities of an organization's Board of Directors as this is the only group who can perform governance activities.

☒ The act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations.

[Report Error](#)

Q. 16 Understanding the current culture and context in which the organization operates is necessary to *

- ☒ Ensure that the GRC capability will operate successfully within the current conditions and to find what could be improved to better support desired organizational outcomes

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) It is essential to understand the context and culture of the organization, as well as the needs and requirements of the various stakeholders, in order to create and maintain a GRC capability appropriately tailored to the organization.

- ☐ Know where to apply stronger controls and oversight because of weak ethical culture

- ☐ Determine what training is needed to improve ethical culture in the organization

- ☐ Be able to identify potential risks in the current external context

Report Error

Q. 17 In an effort to provide a consistent and a repeated organizational commitment to integrity, compliance, and risk management across the organization: *

- ☐ Organizational leaders must set the tone from the bottom-up

- ☒ Organizational leaders must set the tone at the top

Explanation:- According to OCEG GRC Capability Model (Red Book) Leadership must set the tone at the top in both words and deeds to provide consistent and repeated commitment to the organization's established cultural norms and integrity

- ☐ Organizational leaders must set the tone in a Participative approach

- ☐ Organizational leaders must set the tone based on Doctrinal approach

Report Error

Q. 18 When reviewing an organization's culture, one must understand the existing culture including the organizational climate and individual mindsets about *

☐ Key business units, key departments, and key job families and roles.

☐ Industry forces, market forces, and technology forces.

☒ Integrity, compliance, risk and approach to management.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Understand the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance.

☐ Stakeholder needs and requirements.

[Report Error](#)

Q. 19 A mission / vision / values statement is best defined as *

☐ An oral statement made by the CEO to the workforce about the organization's plans for the future

☒ A description of the core beliefs and principles, main aims, intended future state, and overall plan that guides the organization's actions and inspires its people to act toward that future state

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Define Mission, Vision, and Values – Create a formal statement of what the organization will do, what it seeks to be, and the core values the organization holds and applies to its decisions, with commitment from the governing authority and management.

☐ A statement of the key steps that the organization must take to achieve the vision of the GRC capability

☐ A description of principles that the organization has established and about which it provides training

[Report Error](#)

Q. 20 One element of monitoring external context includes *

- ☐ Monitor changes in personnel.
- ☐ Monitor changes in business strategy such as the organization's expansion into new markets.
- ☐ Monitor significant changes in business strategy such as new product development
- ☒ Monitoring geopolitical changes in all relevant areas of operation.

Explanation:- According to OCEG GRC Capability Model (Red Book) Analyze influencing factors in the external context including: Industry forces, Market, Technology, Geopolitical, Environmental and Third-party relationships.

[Report Error](#)

Q. 21 Which of these is NOT a way to assess risk culture? *

- ☐ Ask the workforce whether leadership and management model appropriate risk decision-making and conduct
- ☒ Define the desired state of risk climate and perception indicators

Explanation:- As per the OCEG GRC Capability Model (Red Book) Analyze the existing climate and individual mindsets about how the workforce perceives risk, its impact on their work and the organization as a whole, and how effectively risk management is integrated with the decision-making and running of the business and not the desired state.

- ☐ Identify and categorize risks facing the organization
- ☐ Determine if leadership communicates the risk appetite of the organization to management and the workforce

[Report Error](#)

Q. 22 Which of the following may cause failure of the GRC capability to meet its objectives? *

- ☐ Designing a GRC capability that operates within the existing internal context and operating model of the organization
- ☐ Designing a GRC capability that is responsive to internal stakeholder needs instead of maintaining independence
- ☐ Designing a GRC capability that is consolidated at the top level of the organization
- ☒ Designing a GRC capability that stands apart from mainline operations of the organization to ensure independence.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Design & Implementation Considerations include integrating the management of reward, risk, and compliance and embedding within existing, mainline processes enhance ownership throughout the organization

[Report Error](#)

Q. 23 Which of the following practices should be performed to understand the organization's existing culture? *

- ☒ Analyze ethical leadership, Board involvement, and management style.

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Analyze the existing approach to governing the organization, including the degree to which the governing authority is engaged, and whether leadership sets an appropriate "tone at the top" and models behavior in both words and deeds; the way that policies are used to create management boundaries and how limits are set.

- ☐ Foster ethical leadership, develop incentive based evaluation and promotion decisions, and develop reward programs.
- ☐ Define GRC capability scope, define GRC capability style and goals, and analyze commitment to the GRC capability.
- ☐ Identify compliance risks, operational risks, and economic risks.

[Report Error](#)

Q. 24 When analyzing the internal context of the organization, the GRC capability should consider all of the following EXCEPT: *

☒ IT budgets

Explanation:- According to OCEG GRC Capability Model (Red Book) Analyze influencing factors in the internal context including: Internal strengths and weaknesses (as part of SWOT), Existing strategic plan, Existing operating plan, Existing organizational structures, Existing incentives (appropriate or perverse) for performance, Existing key processes and resources (people, financial, process and technology) and Existing information and gaps or conflicts in information

☐ Key processes and resources

☐ Operating plans

☐ Incentives

[Report Error](#)

Q. 25 Which of the following would be a mistake when developing a stakeholder relations plan? *

☒ Not defining how various stakeholder communications may interact or contradict each other or internal communications

Explanation:- As per the OCEG GRC Capability Model (Red Book) To develop stakeholder relations plan, determine who delivers, responds to, and interacts with each stakeholder type or stakeholder group.

☐ Not using the same form and content of communication for all stakeholder groups

☐ Not having all external stakeholder communications made by legal representatives

☐ Not having the CEO always be the "face" of the organization

[Report Error](#)

Q. 26 One common source of failure related to monitoring the context of an organization is *

- ☐ Analyzing general risk associated with internal and external context to determine whether the risk level associated with the GRC capability is appropriate.
- ☒ Not taking a sufficiently broad view of which external events may apply to the organization.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) A broad view of external events which may apply to the organization is essential to prevent failure related to monitoring the context of an organization

- ☐ Analyzing key areas in the internal and external context in which individuals might attempt to commit fraud.
- ☐ Analyzing key policies in the internal and external context that support the GRC capability.

[Report Error](#)

Q. 27 Which of the following statements about stakeholders is incorrect? *

- ☒ The organization has no ability to influence stakeholders, since they are external to the organization

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Stakeholder requirements can be influenced or change when stakeholders understand the implications to individual businesses, the industry, the economy, and the community at large and the organization understands what motivates the stakeholders (individually and collectively).

- ☐ Organizations should develop key champions within stakeholder groups
- ☐ Not all stakeholders have equal influence
- ☐ Stakeholders are self-legitimizing

[Report Error](#)

Q. 28 For an organization's GRC capability to be successful it must first gain a good understanding of the organization's: *

- ☐ Enterprise-wide technology infrastructure, including the culture in which the organization is currently operating
- ☒ Internal and external business context, including the culture in which the organization is currently operating

Explanation:- According to OCEG GRC Capability Model (Red Book) Understanding the external and internal contexts within which an organization operates, and the culture of the organization, is a critical first step in determining organizational objectives, strategies and structures.

- ☐ Contractual, legal and regulatory requirements, including the culture in which the organization is currently operating
- ☐ The organization's policies and internal control procedures

[Report Error](#)

Q. 29 Many roles have a direct responsibility for GRC activities. Which of the following has less direct responsibility than the others?

- ☐ Chief Information Officer
- ☒ Chief Sales Officer
- ☐ Chief Risk Officer
- ☐ Chief Compliance Officer

[Report Error](#)

Q. 30 According to the Red Book, which of the following is a Universal Outcome of Principled Performance

- ☐ Assess Value of the Organization
- ☐ Increase Corrective Controls
- ☐ Develop Improvement Plan
- ☐ Improve Responsiveness and Efficiency

☒ None of the listed options

Explanation:- None of the options listed is a Universal Outcome of Principled Performance according to the Red Book. The four universal outcomes of principled performance according to the Red Book are: 1. Trust 2. Reputation 3. Ethical Conduct 4. Legal Compliance

[Report Error](#)

Q. 31 Governance can be performed by all of the following groups EXCEPT:

- ☐ IT Steering Committee
- ☐ Board of Directors
- ☐ Audit Committee

☒ Project Committee

[Report Error](#)

Q. 32 Allocate GRC roles and responsibilities to individuals and committees with other roles while ensuring:

☒ Required objectivity and independence

Explanation:- Allocating GRC (Governance, Risk and Compliance) roles and responsibilities is a crucial task for any organization to ensure effective management of risks, compliance with regulations and achievement of business objectives. The individuals and committees with these roles should have the necessary knowledge, skills, and expertise to carry out their responsibilities effectively. Option 2, "Required objectivity and independence" is the correct answer. This is because individuals and committees responsible for GRC should be objective in their assessments and free from conflicts of interest. They should not be influenced by personal biases or have any vested interests that could impact their decision-making. Having an independent oversight function within the organization is important for ensuring objectivity and independence. This function can be achieved through the establishment of a dedicated GRC team or by assigning the GRC responsibilities to individuals or committees who do not have any direct involvement in the areas being monitored.

☐ Transparency of practices and activities

☐ Effectiveness of their control environment

☐ Focus on objectives assigned to their primary roles

[Report Error](#)

Q. 33 Detective controls should

☐ Establish mechanisms for identifying and analyzing risks

☐ Discourage errors or prevent irregularities from occurring

☐ Set the tone for the organization, influencing the control consciousness of its people

☒ Detect actual adverse events and indications of opportunity for any potential adverse events

[Report Error](#)

Q. 34 Which of the following are the three key management actions and controls described in the Notification element of the GRC Capability Model (Red Book)?

- ☐ Capture notifications, investigation, and remediation
- ☐ Capture notifications, respond and resolve and inform and integrate
- ☒ Capture notifications, filter and route notifications, and adhere to data protection requirements
- ☐ Detective controls, filter and route, and code of conduct

[Report Error](#)

Q. 35 Which of the following is NOT a key management action in the Design element?

- ☐ Develop key indicators
- ☐ Explore options to address requirements
- ☒ Analyze risk / reward
- ☐ Design transfer and risk financing strategies

[Report Error](#)

Q. 36 Which of the following objectives is NOT included as measurable GRC capability goals, indicators, thresholds or tolerances?

☒ Provide for an internal enforcement agency

☐ Improve responsiveness and efficiency

☐ Prepare and protect organization

☐ Enhance organizational culture

[Report Error](#)

Q. 37 Which of the following is a key management action in the identification element?

☒ All of these

Explanation:- In the context of risk management, the identification element involves the identification of threats, vulnerabilities, and assets that could be affected by risks. Key management actions in this element include reviewing capability, applying decision-making criteria, addressing inherently high risk, and prioritizing the management of threats, opportunities, and requirements. Option 1: Review capability refers to the management action of reviewing the organization's ability to identify and manage risks. Option 2: Apply decision-making criteria refers to the management action of establishing criteria that will be used to make decisions about how to manage risks. Option 3: Address inherently high risk refers to the management action of addressing risks that are inherently high due to the nature of the organization's operations, assets, or environment. Option 4: Prioritize management of threats, opportunities, and requirements refers to the management action of prioritizing the management of risks based on their potential impact on the organization and its objectives. Therefore, option 1, 2, 3 and 4 are all key management actions in the identification element of risk management.

☐ Review capability

☐ Address inherently high risk

☐ Prioritize management of threats, opportunities and requirements

☐ Apply decision-making criteria

Q. 38 Which of the following approaches will be the most effective in relation to obtaining input from senior executives to conduct scope risk analysis activities?

☐ Sequential analysis

☐ Bottom-up analysis

☒ Top-down analysis

☐ Systemic analysis

[Report Error](#)

Q. 39 Which of the following is NOT a component of the OCEG GRC Capability Model?

☐ Review

☐ Perform

☒ Proact

☐ Learn

[Report Error](#)

Q. 40 Decision-making criteria set by the organization's governing authority include all of the following EXCEPT:

☐ Risk tolerance

☐ Risk appetite

☐ Risk capacity

☒ Risk acceptance

[Report Error](#)

Q. 41 Which one of the following approaches will be the most effective in relation to the participation from the workforce and various line managers to assist in gathering information about what "really happens" in the business, and the risks that the workforce and agents actually face?

☐ Sequential

☐ Systemic

☐ Top-down

☒ Bottom-up

[Report Error](#)

Q. 42 What is not a part of Align element of GRC capability model 3.0

☒ Communication

☐ Direction

☐ Design

☐ Objective

[Report Error](#)

Q. 43 What is not a part of Review element of GRC capability model 3.0

☐ Monitoring

☐ Assurance

☒ Design

☐ Improvement

[Report Error](#)

Q. 44 What includes providing the direction and decision-making criteria that managers and auditors will use in performance of their duties (mission, vision, values, risk appetite, risk tolerances and capacities, ethical guidelines, and a high-level statement of goals and objectives

☐ Objective

☐ Performance

☒ Oversight

☐ Governance

[Report Error](#)

Q. 45 Whose role is to provide oversight distinct from the direction and control provided by those managing the entity or activity being governed

☒ Governing Authority

☐ CFO

☐ Risk Executive and Managers

☐ Compliance and Ethics Executive and Managers

[Report Error](#)

Q. 46 What is an effective integrated GRC capability

☐ creating standardized procedures and templates for things such as policies and training

☒ All of these

☐ establishing common repositories for data, documents, and information

☐ unified vocabulary and taxonomies for information

[Report Error](#)

Q. 47 What is a point of view and approach to business that helps organizations reliably achieve objectives while addressing uncertainty and acting with integrity

☐ Performance

☒ Principled Performance

☐ Governance

☐ Oversight

[Report Error](#)

Q. 48 What is the act of objectively evaluating an entity, process or resource

☐ Governance

☒ Assurance

☐ Oversight

☐ Performance

[Report Error](#)

Q. 49 What is the act of externally directing, controlling and evaluating an entity, process or resource

☐ Performance

☐ Oversight

☐ Objective

☒ Governance

[Report Error](#)

Q. 50 What refers to a measure of the degree to which an objective is achieved relative to a target

☐ Objective

☐ Governance

☒ Performance

☐ Oversight

[Report Error](#)

Q. 51 What is an explicit goal that can be measurably achieved

☒ Objective

☐ Performance

☐ Governance

☐ Oversight

[Report Error](#)

Q. 52 What is an event or condition that has, on balance, an undesirable effect on achieving objectives

☐ Risk

☐ Accident

☐ Oversight

☒ Threat

[Report Error](#)

Q. 53 What is a document that sets out the strategy, structures, processes, activities and resources to appropriately manage the organization's risks to reduce or avoid adverse effects and grasp opportunities

☐ Compliance Management Action Plan

☒ Risk Management Action Plan

☐ Performance Management Action Plan

[Report Error](#)

Q. 54

Organizations that have an integrated GRC capability have seen tangible results from their efforts.

Which of the following is NOT considered as part of tangible results?

- ☒ The ability to improve organizational profitability
- ☐ Top to bottom accountability for key objectives, risks, requirements and related initiatives
- ☐ Improved alignment of objectives with mission, vision and values of the organization
- ☐ Capital allocation to the right initiatives at the right time

Report Error

Q. 55 Which of the following is NOT a component of the OCE GRC Capability Model?

- ☐ Align
- ☐ Perform
- ☐ Learn
- ☒ Context

Report Error

Q. 1 When identifying key external stakeholders for the purpose of analyzing external stakeholder and influencer needs, management should consider the following: *

☒ Shareholders, ratings agencies and media.

Explanation:- As per the OCEG GRC Capability Model (Red Book) Key external stakeholders and influencers, includes Shareholders, Ratings agencies and Media

☐ Ratings agencies, contract employees and media.

☐ Shareholders, key business units and creditors.

☐ Key business units, ratings agencies and suppliers.

[Report Error](#)

Q. 2 A common source of failure in attempts to understand the impact of the External Context would be *

☒ Not relying upon trade associations for information about changes in external context for the industry because they have the resources to do this well

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Factors in the external business context that can affect the organization's ability to meet its objectives includes Industry forces (competitors, supply chain, labor markets, customers, etc.);

☐ Spending time reviewing media reports about the organization or the industry because they are often inaccurate or not timely

☐ Assessing the external context continually instead of on a regular schedule because this is a waste of resources that could be applied elsewhere

☐ Not analyzing how changes in the external context can affect various aspect of GRC capability design and performance

[Report Error](#)

Q. 3 Why is it most important to understand the internal context? *

- ☐ To make sure that those with GRC responsibilities have senior management roles in the organization
- ☐ To know who has what role in the organization and how they can each help the GRC capability
- ☒ To ensure that the GRC capability is designed to align with organizational objectives and existing people, processes and technology

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) To analyze the internal context, involves identify and outline key assets in human capital, technology, physical materials/locations, and information.

- ☐ To know what technology assets may be available to the GRC capability

[Report Error](#)

Q. 4 Understanding the ever-changing external business context is critical to designing a GRC capability that *

- ☐ Is resilient to change and can evolve with it.
- ☒ Changes any time the external context changes.

Explanation:- According to OCEG GRC Capability Model (Red Book) Identify triggers for consideration of changes to the integrated capabilities, in response to changes in the external context

- ☐ Resists change, even when the external shareholders' needs change.
- ☐ Is consistent and does not change when the external environment changes.

[Report Error](#)

Q. 5 Organizational culture is: *

- ☐ The organization's approach to ethics and establishment of principles
- ☐ The behaviour of the organization based on its stated policies
- ☐ The way in which people within the organization exercise ethical judgement and make decisions
- ☒ The existing climate and individual mindsets of those within the organization regarding responsible behavior and integrity, approach to risk, governance style and attitudes about workforce

Explanation:- As per the OCEG GRC Capability Model (Red Book) To enhance organizational culture is to inspire and promote a culture of performance, accountability, integrity, trust, and communication.

[Report Error](#)

Q. 6 A GRC Strategic Plan should include which of the following? *

- ☐ Processes for conducting investigations, providing training and distributing policies
- ☐ Structures and processes for managing GRC information
- ☐ A classification system for risks, identification of sources of risks, and mapping to controls for each key risk
- ☒ Outcomes and maturity milestones, a measurement strategy, and plans for implementation

Explanation:- A GRC Strategic Plan should include outcomes and maturity milestones, a measurement strategy, and plans for implementation. This will help the organization to identify its goals and objectives, determine how to measure progress and success, and develop a plan to implement the necessary changes to achieve those goals.

[Report Error](#)

Q. 7 Risk is considered unacceptably high if *

- ☒ The level of residual risk exceeds the organization's risk tolerance

Explanation:- As per the OCEG GRC Capability Model (Red Book) Explore options to address risk, when the current residual risk is unacceptable

- ☐ The level of residual risk exceeds the organization's risk appetite

- ☐ The level of inherent risk exceeds the organization's risk tolerance

- ☐ The level of inherent risk exceeds the organization's risk appetite

[Report Error](#)

Q. 7 Risk is considered unacceptably high if *

- ☒ The level of residual risk exceeds the organization's risk tolerance

Explanation:- As per the OCEG GRC Capability Model (Red Book) Explore options to address risk, when the current residual risk is unacceptable

- ☐ The level of residual risk exceeds the organization's risk appetite

- ☐ The level of inherent risk exceeds the organization's risk tolerance

- ☐ The level of inherent risk exceeds the organization's risk appetite

[Report Error](#)

Q. 8 Principled Performance represents achievement of:

- ☐ senior management supported objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
- ☐ all of the objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
- ☐ fully funded objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives
- ☒ the most critical objectives that an organization chooses to pursue whilst employing an effective, efficient and responsive approach to governance, risk management and compliance that supports those objectives

[Report Error](#)

Q. 9 Which of the following should be the FIRST step in planning an IT governance implementation?

- ☐ Identify business drivers.
- ☒ Define key business performance indicators.
- ☐ Assign decision-making responsibilities.
- ☐ Obtain necessary business funding.

[Report Error](#)

Q. 10 The BEST way to manage continuous improvement of governance-related processes is to:

- ☒ assess existing process resource capacities.
- ☐ apply effective quality management practices.
- ☐ require third-party independent reviews.
- ☐ define accountability based on roles and responsibilities.

[Report Error](#)

Q. 11 Which of the following is the MOST valuable input when quantifying the loss associated with a major risk event?

- ☐ Business impact analysis (BIA) report
- ☐ IT environment threat modeling
- ☐ Recovery time objectives (RTOs)
- ☒ Key risk indicators (KRIs)

[Report Error](#)

Q. 12 Which of the following is the MOST effective way to manage risks within the enterprise?

☒ Assign individuals responsibilities and accountabilities for management of risks.

☐ Make staff aware of the risks in their area and risk management techniques.

☐ Document procedures and reporting processes.

☐ Provide financial resources for risk management systems.

[Report Error](#)

Q. 13 Internal context analysis should focus on key aspects that drive

☒ organizational value

☐ audit trail

☐ security

[Report Error](#)

Q. 14 Who should provide direction to management so capabilities are designed consistent with decision-making criteria

☐ Risk Executive and Managers

☒ Governing authority

☐ Compliance and Ethics Executive and Managers

☐ CFO

[Report Error](#)

Q. 15 What enables a unified approach to performance, risk, and compliance actions and controls

☐ Determining and defining the KRIs

☐ Determining and defining the KPIs

☒ Determining and defining the risk capacity

[Report Error](#)

Q. 16 Effective objectives are set using

☐ the FIFO method

☒ the SMART model

☐ the LIFO method

[Report Error](#)

Q. 17 What is used to determine if the level of residual risk is acceptable

☐ performance decision-making criteria

☒ Risk decision-making criteria

☐ Compliance decision-making criteria

[Report Error](#)

Q. 18 What will enhance ownership throughout the organization

- ☐ Assessing internal context
- ☒ Integrating the management of reward, risk, and compliance and embedding within existing, mainline processes
- ☐ Making the cultural change

[Report Error](#)

Q. 19 An integrated approach to GRC involves

- ☐ consolidation of the technology infrastructure related to GRC processes.
- ☒ applying a common vocabulary, approach and technology infrastructure to GRC processes.
- ☐ consolidation of the various risk silos.
- ☐ consolidation of governance, risk and compliance processes.

[Report Error](#)

Q. 20 Which is the best description of a Risk Management Action Plan?

- ☐ A plan for how the organization will identify and grasp opportunities presented to it
- ☒ A document that sets out the strategy, structures, processes, activities and resources to appropriately manage the organization's risks to reduce or avoid adverse effects and grasp opportunities
- ☐ A plan that includes the strategy and rationale for addressing each category of risk with particular approaches
- ☐ A document that identifies each risk and its classification by type, source and level of impact

[Report Error](#)

Q. 21 A threat is

- ☐ a measure of likelihood that an adverse event will take place
- ☐ a type of risk
- ☐ always an external force that can harm the organization
- ☒ an event or condition that has, on balance, an undesirable effect on achieving objectives

[Report Error](#)

Q. 22 A GRC Strategic Plan should include which of the following?

- ☒ Outcomes and maturity milestones, a measurement strategy and plans for implementation
- ☐ Processes for conducting investigations, providing training and distributing policies
- ☐ Structures and process for managing GRC information
- ☐ A classification system for risks, identification of sources of risks and mapping to controls for each key risk

[Report Error](#)

Q. 23 Which of the following would NOT be appropriate when monitoring external context?

- ☒ Having only one source of information about each item being monitored
- ☐ Changing approaches to monitoring when entering new markets or geographies
- ☐ Monitoring development of new technologies
- ☐ Identifying a key owner for each aspect of external environment being monitored

[Report Error](#)

Q. 24 Why do you need to analyze the current and planned approaches to addressing opportunities, threats and requirements?

- ☐ To be able to take steps to mitigate entire categories of risks or address entire categories of potential reward
- ☒ To be able to determine if the inherent, actual and planned residual levels of risk, reward and conformance are acceptable
- ☐ To be able to have the same crisis management plan for all risks
- ☐ To be able to assign responsibility for monitoring changes in approaches to risks, rewards and conformance in a given category to one person

Q. 25 Which of the following is NOT true?

- ☒ An organization always should have only one code of conduct that applies to everyone throughout the organization
- ☐ A code of conduct may be required by law, regulation or other authority for certain roles or positions in the organization
- ☐ The code of conduct may contain guidelines for responsible decision-making when the code, other guidance or law is unclear
- ☐ The code of conduct will be ineffective if it is written at a level of language its intended audience does not understand

[Report Error](#)

Q. 26 When establishing procedures for investigating complaints or reports about compliance or ethical issues, an organization must:

- ☐ Define policies and procedures that ensure that such complaints or reports are never handled directly by line management
- ☐ Define policies and procedures to ensure that the board is aware of all compliance or ethical issues
- ☒ Define policies and procedures designed to make sure that the confidentiality of all reported information is protected

Explanation:- Answer: When establishing procedures for investigating complaints or reports about compliance or ethical issues, an organization must define policies and procedures designed to make sure that the confidentiality of all reported information is protected. Explanation: Protecting the confidentiality of reported information is crucial to ensuring that employees feel safe and comfortable reporting any issues that arise. If employees feel that their confidentiality is not protected, they may be hesitant to report compliance or ethical issues, which could lead to larger problems for the organization. Therefore, an organization must establish policies and procedures that ensure that the confidentiality of reported information is protected. Option 2 is incorrect because while it is important for the board to be aware of compliance or ethical issues, defining policies and procedures for this purpose alone is not sufficient. Option 3 is incorrect because while it is important to escalate significant issues to senior management and/or outside counsel immediately upon validation, this is only one part of the process. Option 4 is incorrect because it is not always feasible for complaints or reports to be handled directly by senior management, and therefore, organizations must establish policies and procedures that allow for the appropriate handling of such issues by line management.

Q. 27 Which of the following would not be considered an external stakeholder or influencer of opinion?

☐ Local media in areas where the organization operates

☐ Regulators

☐ A non-governmental organization

☒ The Board of Directors

[Report Error](#)

Q. 28 Why is it important to establish formal values and objectives for the organization?

☐ In the absence of organizational values and objectives, legal mandates will replace the organization's right to establish its own values

☒ Absent a clear mission, vision and values statement, the organization will operate on the values defined ad hoc or by individuals based on their own beliefs and interests

☐ Organizational values and objectives provide a defense to charges that the organization does not have an effective compliance program.

☐ A written values statement can substitute for leadership demonstrating the desired behavior of the workforce.

[Report Error](#)

Q. 29 Which of the following is a potential source of failure when establishing an approach to integrate and align the GRC capability with the business?

- ☐ re--using technologies that are already serving needs in the organization for some aspects of the GRC capability, rather than putting all new technology in place that is designed to manage and analyze GRC information
- ☒ viewing establishment or alteration of the GRC capability as a change activity that requires special management rather than it being just a part of ongoing business
- ☐ not assigning clear accountability for all key aspects of the GRC capability
- ☐ establishing a centralized system for maintaining GRC information in a way that it can be accessed by different departments and functions

[Report Error](#)

Q. 30 A common mistake in setting up notification pathways is

- ☒ Not capturing all notifications made via informal methods or unstructured channels.
- ☐ Encouraging stakeholders to raise concerns directly with the organization instead of going directly to external channels.
- ☐ Designing the capability so stakeholders can trust that concerns are taken seriously.
- ☐ Using technology resources as the pathway to provide notification.

[Report Error](#)

Q. 31 What is a GRC curriculum plan?

- ☐ A plan describing what the organization intends to offer as training about GRC to the workforce, for approval by the board
- ☐ A plan setting out the names of all courses and training programs offered to the workforce by the organization
- ☐ A table of contents for the organization's training course about the GRC capability
- ☒ A plan setting out the order and timing of all courses for a particular role or family of roles, which may include a description of each course, its objectives, and method/mode of delivery

[Report Error](#)

Q. 32 What can be achieved by applying Principled Performance

- ☒ All of these
- ☐ the most critical objectives that an organization chooses to pursue
- ☐ employing an effective, efficient and responsive approach to risk management and compliance that supports those objectives
- ☐ employing an effective, efficient and responsive approach to governance supporting those objectives

[Report Error](#)

Q. 33 What are proactive actions and controls?

- ☐ Specified process steps or actions that will allow the organization to identify misconduct as it occurs
- ☒ Specified process steps or actions that will reduce the likelihood and impact of undesirable events, activities or behavior
- ☐ Technology controls that detect the opportunity for misconduct or adverse events and prevent them from occurring
- ☐ Technology and processes that help the organization to correct any detected instances of misconduct before an adverse impact arises

[Report Error](#)

Q. 34 Which of the following statements is NOT correct?

- ☒ Assurance should be performed by individuals who have the deepest understand of the actions and controls.
- ☐ Assurance desired may vary at different times and for different purposes.
- ☐ Assurance should focus on the ability of the GRC capability to meet its objectives while being consistent to the decision-making criteria.
- ☐ Assurance efforts are most effective when a risk based approach is used.

[Report Error](#)

Q. 35 What is the benefit of Principled Performance to organizations

- ☐ Able to honor mandatory commitments including legal compliance
- ☐ reliably achieve objectives while addressing uncertainty and acting with integrity
- ☒ All of these
- ☐ It enables performance while considering both threats and opportunities

[Report Error](#)

Q. 36 Who must help managers perform better by establishing and explaining decision-making criteria related to the financial mindset of the organization

- ☐ Risk Executive and Managers
- ☐ Governing authority
- ☐ Compliance and Ethics Executive and Managers
- ☒ CFO

[Report Error](#)

Q. 37 Who drives Principled Performance by selectively establishing and supporting business improvement initiatives

☒ CFO

☐ Risk Executive and Managers

☐ Governing authority

☐ Compliance and Ethics Executive and Managers

[Report Error](#)

Q. 38 Who sets the mission

☐ CFO

☐ Risk Executive and Managers

☒ Governing authority

☐ Compliance and Ethics Executive and Managers

[Report Error](#)

Q. 39 Who sets the vision and values

☒ Governing authority

☐ CFO

☐ Risk Executive and Managers

☐ Compliance and Ethics Executive and Managers

[Report Error](#)

Q. 40 Who sets the risk appetite, risk tolerances and capacities

☐ Risk Executive and Managers

☒ Governing authority

☐ Compliance and Ethics Executive and Managers

☐ CFO

[Report Error](#)

Q. 41 Who sets the ethical guidelines

☐ Risk Executive and Managers

☒ Governing authority

☐ Compliance and Ethics Executive and Managers

☐ CFO

[Report Error](#)

Q. 42 Who sets the a high-level statement of goals and objectives

☒ Governing authority

☐ Compliance and Ethics Executive and Managers

☐ CFO

☐ Risk Executive and Managers

[Report Error](#)

Q. 43 What is the core task of governing authority

☐ to ensure that any fluctuation that arises due to changes in the internal or external context is evaluated to determine how changes may impact achievement of objectives

☒ to provide oversight

☐ to ensure satisfying internally established values, policies, procedures, and codes of conduct

☐ to ensure understanding an appropriate distribution of financial resources throughout the business

[Report Error](#)

Q. 44 The task of a Chief Financial Officer, is

- ☒ to ensure understanding an appropriate distribution of financial resources throughout the business
- ☐ to provide oversight
- ☐ to ensure satisfying internally established values, policies, procedures, and codes of conduct
- ☐ to ensure that any fluctuation that arises due to changes in the internal or external context is evaluated to determine how changes may impact achievement of objectives

[Report Error](#)

Q. 45 Which of the following is the task of risk executive and managers

- ☐ to ensure satisfying internally established values, policies, procedures, and codes of conduct
- ☐ to ensure understanding an appropriate distribution of financial resources throughout the business
- ☒ to ensure that any fluctuation that arises due to changes in the internal or external context is evaluated to determine how changes may impact achievement of objectives
- ☐ to provide oversight

[Report Error](#)

Q. 46 What is the task of compliance and ethics executive and managers

- ☐ to ensure understanding an appropriate distribution of financial resources throughout the business
- ☒ to ensure satisfying internally established values, policies, procedures, and codes of conduct
- ☐ to ensure that any fluctuation that arises due to changes in the internal or external context is evaluated to determine how changes may impact achievement of objectives
- ☐ to provide oversight

[Report Error](#)

Q. 47 What is the core task of chief information executive and managers

- ☐ to establish the culture of the hiring
- ☒ to design the GRC technology strategic plan
- ☐ have day-to-day responsibility to identify and manage risks directly as they arise in the business operations
- ☐ to assess the effectiveness of the design of risk and compliance systems

[Report Error](#)

Q. 47 What is the core task of chief information executive and managers

- ☐ to establish the culture of the hiring
- ☒ to design the GRC technology strategic plan
- ☐ have day-to-day responsibility to identify and manage risks directly as they arise in the business operations
- ☐ to assess the effectiveness of the design of risk and compliance systems

[Report Error](#)

Q. 48 The task of human resources executive and managers, is

- ☐ to assess the effectiveness of the design of risk and compliance systems
- ☐ have day-to-day responsibility to identify and manage risks directly as they arise in the business operations
- ☐ to design the GRC technology strategic plan
- ☒ to establish the culture of the hiring

[Report Error](#)

Q. 49 Which of the following is the task of internal audit executive and managers

- ☐ to design the GRC technology strategic plan
- ☒ to assess the effectiveness of the design of risk and compliance systems
- ☐ have day-to-day responsibility to identify and manage risks directly as they arise in the business operations
- ☐ to establish the culture of the hiring

[Report Error](#)

Q. 50 What is the task of business unit operator and managers

- ☐ to assess the effectiveness of the design of risk and compliance systems
- ☐ to design the GRC technology strategic plan
- ☒ have day-to-day responsibility to identify and manage risks directly as they arise in the business operations
- ☐ to establish the culture of the hiring

[Report Error](#)

Q. 51 Who establishes the culture of the compensation in organization

- ☐ business unit operator and managers
- ☐ chief information executive and managers
- ☐ internal audit executive and managers
- ☒ human resources executive and managers

[Report Error](#)

Q. 52 Who establishes the culture of incentives in organization

- ☒ human resources executive and managers
- ☐ business unit operator and managers
- ☐ chief information executive and managers
- ☐ internal audit executive and managers

[Report Error](#)

Q. 53 Who is responsible to discipline the employees in organization

☐ internal audit executive and managers

☒ human resources executive and managers

☐ business unit operator and managers

☐ chief information executive and managers

[Report Error](#)

Q. 54 Who is referred to as the “first line of defense” in organizational risk management

☐ human resources executive and managers

☐ chief information executive and managers

☐ internal audit executive and managers

☒ business unit operator and managers

[Report Error](#)

Q. 55 How many universal outcomes of principled performance are listed under GRC capability model 3.0

☐ 11

☐ 9

☐ 8

☒ 10

[Report Error](#)

Q. 56 Which capability under the GRC Capability Model examines and analyzes context and culture

☐ P – PERFORM

☒ L – LEARN

☐ A – ALIGN

☐ R – REVIEW

[Report Error](#)

Q. 57 Which of the following is an element of governance?

☒ Building plans to align with the direction set by the governance body

☐ Evaluating stakeholder needs to determine enterprise objectives

☐ Monitoring activities designed to achieve enterprise objectives

[Report Error](#)

Q. 58 Which of the following BEST enables an enterprise to maximize value from the use of I&T?

☒ An actionable strategy and governance system

☐ Well-documented and monitored business processes

☐ A clearly defined I&T management structure

[Report Error](#)

Q. 1 One common mistake when watching the external and internal context of an organization is *

- ☐ Spending so much time monitoring high risks that the company cannot allocate enough resources to monitoring low risk areas.
- ☒ Not monitoring inherently high risks because of a belief that controls will not fail or that the occurrence is unlikely.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) A common mistake when watching the external and internal context of an organization is not monitoring inherently high risks because of a belief that controls will not fail or that the occurrence is unlikely.

- ☐ Having multiple channels to identify significant changes to the context
- ☐ Assigning responsibility for tracking each aspect to identify and analyze changes.

[Report Error](#)

Q. 2 One common mistake made understanding the internal context of an organization is *

- ☐ Not assigning accountability for implementing or maintaining optimizing activities and assuming it will just get done.
- ☐ Not understanding the needs of shareholders, thus not including these needs in the GRC capability.
- ☒ Not considering the internal context and existing operating model when designing the GRC capability, thus designing a capability that stands apart from mainline operations.

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Analyze influencing factors in the internal context includes , Internal strengths and weaknesses (as part of SWOT), Existing strategic plan, Existing operating plan, Existing organizational structures, Existing incentives (appropriate or perverse) for performance, Existing key processes and resources (people, financial, process and technology), Existing information and gaps or conflicts in information

- ☐ Not understanding the organization's weakness in ability to effectively and efficiently react to changes in the community.

[Report Error](#)

Q. 3 Which of the following is NOT a key step in Identifying risks that may affect the organization? *

- ☐ Identify risks that may afford opportunities for the organization
- ☐ Identify business objectives and operations that may be affected
- ☒ Identify the tactics to be applied to mitigate risks

Explanation:- According to OCEG GRC Capability Model (Red Book) In Identifying risks, tactics to be applied to mitigate risks is not included

- ☐ Identify risks of noncompliance with legal mandates and internal policies

[Report Error](#)

Q. 4 What is a segregation of duties document? *

- ☐ A document which states that roles with an interest in uncovering misconduct must be separated from roles that have an interest in business performance objectives
- ☒ A document that sets out which, responsibilities or roles must not be assigned to a person with certain other responsibilities or roles as a protective measure to prevent fraud, error or conflict of interest

Explanation:- As per the OCEG GRC Capability Model (Red Book) Segregation of Duties documents is a document reflecting that the responsibilities of some roles or positions should be kept distinct from the responsibilities of other roles or positions as a protective measure to prevent fraud, error, or conflict of interest

- ☐ A document that sets out the organizational structure of the GRC capability with each role identified
- ☐ A document that states which people in the organization must not participate in certain decisions

[Report Error](#)

Q. 5 For an organization to effectively achieve its business objectives, and to operate under the values for which it stands for, it is imperative for the organization to: *

☒ Align organizational business objectives to mission, vision and values

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Align organizational business objectives to mission, vision and values

☐ Align organizational business objectives to organizational roles and responsibilities

☐ Align organizational business objectives to organizational optimal performance management

☐ Align organizational business objectives to organizational technology infrastructure

[Report Error](#)

Q. 6 Which one of the following help most to facilitate the adoption and acceptance of the organization's GRC capability? *

☒ Organizational GRC capability support team

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Organizational GRC capability support team facilitate the adoption and acceptance of the organization's GRC capability

☐ Organizational inquiries and investigations team

☐ Organizational leaders and champions team

☐ Organizational internal communications team

[Report Error](#)

Q. 7 Which of these is NOT an appropriate step to take in creation and management of the values statement of the organization? *

- ☒ Prevent the values statement from being viewed by anyone outside of the organization because that may lead to challenges

Explanation:- According to OCEG GRC Capability Model (Red Book) The values statement should be viewed by anyone outside of the organization

- ☐ Periodically review the need for changes to the values statement based on changes in the internal and external context
- ☐ Revisit the values statement when engaged in a merger or acquisition activity
- ☐ Involve the Board in developing the values statement, in addition to a range of internal stakeholders

[Report Error](#)

Q. 8 Which one of the following approaches will be the most effective in relation to obtaining input from senior executives to conduct scope risk analysis activities? *

- ☐ Bottom-up analysis

- ☒ Top-down analysis

Explanation:- As per the OCEG GRC Capability Model (Red Book) Top-down analysis and input from senior executives to scope analysis activities.

- ☐ Systemic analysis
- ☐ Sequential analysis

[Report Error](#)

Q. 9 Decision-making criteria set by the organization's governing authority include all of the following EXCEPT: *

☐ Risk tolerance

☐ Risk capacity

☐ Risk appetite

☒ Risk acceptance

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Risk decision-making criteria (e.g. risk appetite, tolerance, and capacity) are used to determine if the level of residual risk is acceptable and that the established targets of reward are commensurate with the acceptable risk levels.

[Report Error](#)

Q. 10 Which one of the following approaches will be the most effective in relation to the participation from the workforce and various line managers to assist in gathering information about what "really happens" in the business, and the risks that the workforce and agents actually face? *

☐ Top-down

☐ Sequential

☒ Bottom-up

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Bottom-up analysis sends information from business operations, used together ensure the analysis reflects operational reality.

☐ Systemic

[Report Error](#)

Q. 11 Which of the following components of a governance system are MOST likely to be underestimated as factors in the success of governance and management activities?

☐ Principles, policies and frameworks

☒ Culture, ethics and behavior

☐ People, skills and competencies

[Report Error](#)

Q. 12 Which of the following components of the governance system are required for successful completion of all activities?

☒ People, skills and competencies

☐ Principles, policies and frameworks

☐ Processes

[Report Error](#)

Q. 13 Which of the following is a CRITICAL requirement when the IT function is strategic and crucial to the success of the business?

☐ Highly capable security-related processes and ensured risk optimization

☐ High involvement of IT-related roles in organizational structures

☒ Documented IT policies and procedures

[Report Error](#)

Q. 14

An enterprise that specializes in software development is designing a new IT governance system as part of a transition from traditional waterfall to a more agile approach.

Which step in the design phase would this transition impact the MOST?

☐ Compliance requirements

☐ Sourcing model

☒ Implementation method

[Report Error](#)

Q. 15

The CEO of a large enterprise has announced the commencement of a major business expansion that will double the size of the organization. IT will need to support the expected demand expansion.

The CIO should FIRST:

☐ update the IT strategic plan to align with the decision.

☒ review the resource utilization matrix.

☐ embed IT personnel in the business units.

☐ recruit IT resources based on the expansion decision.

[Report Error](#)

Q. 16

A large retail chain realizes that while there has not been any loss of data, IT security has not been a priority and should become a key goal for the enterprise.

What should be the FIRST high-level initiative for a newly created IT strategy committee in order to support this business goal?

☒ Identifying gaps in information asset protection

☐ Recruiting and training qualified IT security staff

☐ Defining data archiving and retrieval policies

☐ Modernizing internal IT security practices

[Report Error](#)

Q. 17

An enterprise has decided to create its first mobile application. The IT director is concerned about the potential impact of this initiative.

Which of the following is the MOST important input for managing the risk associated with this initiative?

☐ IT risk scorecard

☒ Business requirements

☐ Enterprise risk appetite

☐ Enterprise architecture

[Report Error](#)

Q. 18 Which of the following aspects of the transition from X-rays to digital images would be BEST addressed by implementing information security policy and procedures?

- ☐ Training technicians on acceptable use policy
- ☒ Protecting personal health information
- ☐ Establishing data retention procedures
- ☐ Minimizing the impact of hospital operation disruptions on patient care

[Report Error](#)

Q. 19

A multinational enterprise recently purchased a large company located in a different country.

When introducing the concept of governance to the new acquisition, it is MOST important that executive management recognize:

- ☐ the impact of cultural changes.
- ☒ globally recognized good practices.
- ☐ language differences.
- ☐ the use of international standards.

[Report Error](#)

Q. 20 What is a responsive action and control

☐ Communication

☐ Notification

☐ Inquiry

☒ None of these

[Report Error](#)

Q. 21 What is not a detective action and control

☐ Notification

☒ Communication

☐ None of these

☐ Inquiry

[Report Error](#)

Q. 22 What is a Proactive Action and Control

☐ None of these

☒ Communication

☐ Notification

☐ Inquiry

[Report Error](#)

Q. 23 What help people decide what to do in the absence of an explicit policy or procedure

☐ Industry practice and norm

☒ Ethical decision guidelines

Explanation:- Explanation: Ethical decision guidelines help people make decisions when there are no explicit policies or procedures to follow. These guidelines are designed to help individuals identify ethical considerations and make choices that align with their values and those of their organization. Ethical decision guidelines typically include key principles such as honesty, integrity, fairness, and respect for others. They can also include decision-making frameworks, such as the "four-way test," which asks individuals to consider whether their actions are truthful, fair, beneficial, and respectful. By providing a set of principles and tools to guide decision-making, ethical decision guidelines help ensure that individuals and organizations act in an ethical and responsible manner.

☐ Internal and External Context

[Report Error](#)

Q. 24 When do employees are more likely to believe the organization is committed to those values and the desired conduct expectations

☒ When initial hiring criteria reflect the values of the organization

☐ Developing a broad recognition program as stakeholders prefer

☐ Designing simple and transparent compensation

[Report Error](#)

Q. 25 What allows the organization more flexibility to correct action and control weaknesses

☐ Establishing notification pathways

☒ Encouraging stakeholders to raise issues directly with the organization, rather than via external channels

☐ Capturing notifications made via informal methods

[Report Error](#)

Q. 26 What is not a part of Learn element of GRC capability model 3.0

☒ Communication

☐ Culture

☐ External Context

☐ Internal Context

[Report Error](#)

Q. 27

Senior management has made a decision to automate a number of key controls due to concerns that current IT risk controls are overly cumbersome and adversely impacting IT agility.

Which of the following should be required FIRST to facilitate this process?

☐ Controls optimization

☐ Control gap analysis

☐ Control self-assessments

☒ Cost-benefit analysis

[Report Error](#)

Q. 28

A business case indicates an enterprise would reduce costs by implementing a bring your own device (BYOD) program allowing employees to use personal devices for e-mail.

Which of the following should be the FIRST governance action?

☒ Assess the enterprise architecture (EA).

☐ Assess the BYOD risk.

☐ Update the BYOD policy.

☐ Update the network infrastructure.

[Report Error](#)

Q. 29 Which of the following is MOST critical to support governance cultural changes within an organization?

☒ Established monitoring and measuring

☐ IT governance process manuals

☐ Regularly scheduled governance training

☐ Demonstrated management commitment

[Report Error](#)

Q. 31 Which of the following is PRIMARILY achieved through performance measurement?

☒ Process improvement

☐ Cost efficiency

☐ Benefit realization

☐ Transparency

[Report Error](#)

Q. 32 Which of the following would BEST help to ensure timely reporting on risk events and responses to appropriate levels of management?

☐ Emergency response team

☐ Key personnel interviews

☐ Escalation procedures

☒ Corporate directory

[Report Error](#)

Q. 33

An enterprise has entered into a new market which brings additional regulatory compliance requirements.

To address these new requirements, the enterprise should FIRST:

☐ outsource the compliance process.

☐ appoint a compliance officer.

☐ update the organization's risk profile.

☒ have executive management monitor compliance.

[Report Error](#)

Q. 35 Before establishing key risk indicators, which of the following should be defined FIRST?

☐ Risk and security framework

☐ resource strategy

☐ Key performance indicators

☒ Goals and objectives

[Report Error](#)

Q. 36 When conducting a risk assessment in support of a new regulatory requirement, the risk committee should FIRST consider the:

☒ risk profile of the enterprise.

☐ disruption to normal business operations.

☐ readiness of IT systems to address the risk.

☐ cost burden to achieve compliance.

[Report Error](#)

Q. 37 Which of the following is the BEST way to address concerns associated with outsourcing an IT process?

☐ Perform a risk assessment.

☐ Review the IT governance framework.

☐ Manage service levels.

☒ Implement a business continuity plan.

[Report Error](#)

Q. 38 To ensure IT risk is managed in a consistent manner, it is MOST important for IT governance to establish a:

☐ risk management reporting tool to ensure compliance.

☐ risk management framework.

☒ risk management committee to identify IT-related risks.

☐ balanced scorecard that includes IT risks.

[Report Error](#)

Q. 39 The PRIMARY objective of resource planning within an enterprise should be to:

☐ determine risk associated with resources

☐ finalize service level agreements

☐ determine outsourcing options.

☒ maximize value received

[Report Error](#)

Q. 40 Which of the following is the BEST way to implement effective risk management?

☐ Align with business risk management processes.

☐ Establish a risk management function.

☐ Minimize the number of IT risk management decision points.

☒ Adopt risk management processes.

[Report Error](#)

Q. 41 Which of the following is the PRIMARY purpose of an effective set of key risk indicators (KRIs)?

☐ Evaluating existing technology for risk monitoring capabilities

☐ Identifying possible future adverse impacts on the enterprise

☐ Quantifying the productivity of the risk management team

☒ Establishing executive level buy-in of the risk program

[Report Error](#)

Q. 42 Which of the following is the BEST method for determining an enterprise's current appetite for risk?

☐ Evaluating the balanced scorecard

☐ Assessing social media adoption

☒ Interviewing senior management

☐ Reviewing recent audit findings

[Report Error](#)

Q. 43 Which of the following provides the BEST evidence of effective governance?

☒ Comprehensive policies and procedures

☐ Cost savings and human resource optimization

☐ Business value and customer satisfaction

☐ risk identification and mitigation

[Report Error](#)

Q. 44 What is a critical first step in determining organizational objectives

☐ Align performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements.

☒ Understanding the external and internal contexts within which an organization operates

☐ Understand the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance

[Report Error](#)

Q. 45 What is needed to create and maintain a GRC capability appropriately tailored to the organization

- ☒ Understand the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance
- ☐ Align performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements.
- ☐ Understanding the external and internal contexts within which an organization operates

[Report Error](#)

Q. 46 What is critical to designing appropriate objectives, strategies, and resilient capabilities

- ☐ Align performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements.
- ☐ Understand the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance
- ☒ All of the listed options

Explanation:- All three options are critical to designing appropriate objectives, strategies, and resilient capabilities. 1. Understanding the external and internal contexts within which an organization operates is important for identifying opportunities and risks that could affect the organization's objectives and strategies. 2. Understanding the existing culture, including how leadership models culture, the organizational climate, and individual mindsets about the governance, assurance, and management of performance, risk, and compliance, is important for designing strategies and capabilities that align with the organization's values and beliefs. 3. Aligning performance, risk, and compliance objectives, strategies, decision-making criteria, actions, and controls with the context, culture, and stakeholder requirements is important for ensuring that the organization's objectives are met while minimizing risk and ensuring compliance with applicable laws and regulations.

- ☐ Understanding the external and internal contexts within which an organization operates

[Report Error](#)

Q. 47 Which of the following is not a influencing factor in the external context

☐ Third-party relationships

☐ Technology

☐ Regulatory and legal

☒ Existing strategic plan

[Report Error](#)

Q. 48 What is not a influencing factor in the internal context

☐ Existing operating plan

☒ Third-party relationships

☐ Existing strategic plan

☐ Existing organizational structures

[Report Error](#)

Q. 49 Which of the following would BEST mitigate identified vulnerabilities in a timely manner?

- ☐ Continuous vulnerability monitoring tool
- ☐ Categorization of the vulnerabilities based on system's criticality
- ☒ Monitoring of key risk indicators (KRIs)
- ☐ Action plan with responsibilities and deadlines

[Report Error](#)

Q. 50 How does an enterprise benefit from implementing a set of key risk indicators (KRIs)?

- ☐ The frequency of risk data gathering and reporting is minimized.
- ☐ The need for a formal risk and control assessment program is eliminated.
- ☒ Risk exposures are monitored to ensure they remain within risk appetite.
- ☐ The set of KRIs remains relevant over time.

[Report Error](#)

Q. 51 A recent audit of IT investments has found that while initial returns meet expectations, benefits realization declines more than expected over time. Which of the following is the BEST way to address this situation?

☐ Institute project quality and performance metrics.

☐ Standardize resource monitoring approaches.

☐ Establish key risk indicators (KRIs).

☒ Institute regular business case updates and reviews

[Report Error](#)

Q. 52 Which of the following BEST defines the investment activities an enterprise will undertake when aligning to business goals?

☐ Procurement management

☐ Portfolio management

☐ Project management

☒ Risk management

[Report Error](#)

Q. 53

An audit report indicates that a lack of IT employee risk awareness is creating serious security issues in application design and configuration.

Which of the following would be the BEST key risk indicator (KRI) to show progress in IT employee behavior?

- ☒ Number of reported security incidents
- ☐ Results of application security testing
- ☐ Number of IT employees attending security training sessions
- ☐ Results of application security awareness training quizzes

[Report Error](#)

Q. 54 Which of the following is the MOST important reason for selecting IT key risk indicators (KRIs)?

- ☒ Increasing the probability of achieving IT goals
- ☐ Assessing the current IT controls model
- ☐ Demonstrating the effectiveness of IT risk policies
- ☐ Enabling comparison against similar IT KRIs

[Report Error](#)

Q. 55

A large enterprise has decided to use an emerging technology that needs to be integrated with the current IT infrastructure.

Which of the following is the BEST way to prevent adverse effects to the enterprise resulting from the new technology?

☐ Implement service level agreements (SLAs).

☐ Update the risk appetite statement.

☒ Develop key performance indicators (KPIs).

☐ Develop key risk indicators (KRIs).

[Report Error](#)

Q. 56 Which of the following will BEST enable an enterprise to convey IT governance direction and objectives?

☐ Corporate culture

☒ Principles and policies

☐ Skills and competencies

☐ Business processes

[Report Error](#)

Q. 57 When assessing the impact of a new regulatory requirement, which of the following should be the FIRST course of action?

☒ Map the regulation to business processes.

☐ Update affected IT policies.

☐ Assess the budget impact of the new regulation.

☐ Implement new regulatory requirements.

[Report Error](#)

Q. 58 Which of the following BEST indicates that a change management process has been implemented successfully?

☐ Degree of control

☐ Process performance

☒ Outcome measures

☐ Maturity levels



[Report Error](#)

Q. 59 Which of the following BEST enables the alignment of IT and enterprise strategy?

☒ IT resource planning

☐ IT performance monitoring and reporting

☐ Project portfolio management

☐ Enterprise compliance audits

[Report Error](#)

Q. 60 Which of the following should be the PRIMARY goal of implementing service level agreements (SLAs) with an outsourcing vendor?

☐ Establishing penalties for not meeting service levels

☐ Complying with regulatory requirements

☐ Gaining a competitive advantage

☒ Achieving operational objectives

[Report Error](#)

Q. 1 Which aspects of the GRC capability require board involvement? *

☐ Vetting assessment of highest priority risks, monitoring activities performed by senior management, and setting compensation for senior GRC executives

☐ Defining the categories of risks for a risk taxonomy, assessing the operation of GRC controls, and defining job descriptions for key GRC roles

Explanation:- According to OCEG GRC Capability Model (Red Book) The aspects are defining the categories of risks for a risk taxonomy, assessing the operation of GRC controls, and defining job descriptions for key GRC roles

☐ Performing assessment of risks to determine the highest risks, establishing the control activities that senior management may perform, setting compensation for all GRC personnel

☒ Monitoring highest priority risks, defining control activities for highest risks, perform background checks for key GRC personnel

[Report Error](#)

Q. 2 Which of the following objectives is NOT included as measurable GRC capability goals, indicators, thresholds or tolerances? *

☐ Improve responsiveness and efficiency

☐ Enhance organizational culture

☐ Prepare and protect organization

☒ Provide for an internal enforcement agency

Explanation:- As per the OCEG GRC Capability Model (Red Book) Provide for an internal enforcement agency is not included.

[Report Error](#)

Q. 3 Which best describes the key practices in risk assessment? *

- ☐ Analyze the effect of current management approaches for risks, determine the cost to maintain current approaches, determine level of residual risk
- ☐ Analyze inherent risks, identify current approaches to managing each risk, determine current residual risks, prioritize risks that require changes in management approach based on risk appetite
- ☐ Identify and classify risks, list the risks in order of perceived potential negative impact, identify risks to be avoided, control remaining risks
- ☒ Identify for each risk whether it is currently accepted, avoided, shared, or reduced; and identify if reduced risks are managed by preventive, detective or corrective controls

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) In risk assessment, identify for each risk whether it is currently accepted, avoided, shared, or reduced; and identify if reduced risks are managed by preventive, detective or corrective controls

[Report Error](#)

Q. 4 Who is responsible for the establishing the "charter", "purpose" and "goals" of the organization's GRC capability? *

☐ The Organization's Chief Risk Officer

☐ The Organization's Chief Compliance Officer

☒ The Organization's Board of Directors

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) The core task of any governing authority, be it the corporate board or a committee overseeing a particular project, is to provide oversight distinct from the direction and control provided by those managing the entity or activity being governed.

☒ The Organization's Chief Financial Officer

[Report Error](#)

Q. 5 What should be an overriding goal in establishing the organizational structure of the GRC capability? *

- ☐ To have a single point of authority and accountability for the entire GRC capability
- ☒ To ensure that the GRC capability is integrated with the existing operating model of the organization

Explanation:- According to OCEG GRC Capability Model (Red Book) Integrating GRC capabilities is about establishing an approach that ensures the right people get the appropriate and correct information at the right times, that the right objectives are established, and that the right actions and controls necessary to address uncertainty and act with integrity are put in place.

- ☐ To make sure that those with GRC responsibilities have senior management roles in the organization
- ☐ To ensure that the GRC capability is overseen and operated from a centralized department that has enterprise-wide authority

[Report Error](#)

Q. 6 An organization's GRC capability should be directed, designed, operated and evaluated by: *

- ☐ The Organization's Chief Information Officer, business management committees, and external management consultants
- ☐ The Organization's Chief Risk Officer, business management committees, and the GRC consultants
- ☐ The Organization's Chief Compliance Officer, and the various divisional managers across the organization
- ☒ The Organization's Board, senior management, and the individuals at various levels of the organization that are not a part of the management team

Explanation:- As per the OCEG GRC Capability Model (Red Book) The core task of any governing authority, be it the corporate board or a committee overseeing a particular project, is to provide oversight distinct from the direction and control provided by those managing the entity or activity being governed.

[Report Error](#)

Q. 7 Decision-making criteria used in risk management are established by whom? *

☐ Chief Financial Officer

☒ Board of Directors

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) The core task of any governing authority, be it the corporate board or a committee overseeing a particular project, is to provide oversight distinct from the direction and control provided by those managing the entity or activity being governed. Oversight includes providing the direction and decision-making criteria that managers and auditors will use in performance of their duties.

☐ Chief Executive Officer

☐ Chief Risk Officer

[Report Error](#)

Q. 8 The organization's GRC capability will only be effective and successful, if it contributes to the organization's: *

☐ Legal and regulatory objectives

☐ Technology objectives

☒ Business objectives

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) A Universal Outcomes of Principled Performance is Achieve Business Objectives

☐ Compliance objectives

[Report Error](#)

Q. 9 The role responsible for developing the risk framework is the *

☐ Chief Executive Officer

☒ Chief Risk Officer

Explanation:- According to OCEG GRC Capability Model (Red Book) Risk teams both directly under the CRO and within business units must consider threats and opportunities presented to the organization and ensure that this information is available as strategic plans are developed and implemented.

☐ Chief Compliance Officer

☐ Board of Directors

[Report Error](#)

Q. 10 Which of the following is a key management action in the Identification element? *

☐ Apply decision-making criteria

☒ Review capability

Explanation:- As per the OCEG GRC Capability Model (Red Book) Review Capability – Identify and evaluate the existing capability (people, process, and technology) and how it affects ability to achieve objectives.

☐ Address inherently high risk

☐ Prioritize management of threats, opportunities and requirements

[Report Error](#)

Q. 11 Which is the best description of a risk management action plan? *

☐ A document that identifies each risk and its classification by type, source and level of impact

☐ A plan for how the organization will identify and grasp opportunities presented to it

☒ A document that sets out the strategy, structures, processes, activities and resources to appropriately manage the organization's risks to reduce or avoid adverse effects and grasp opportunities

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) risk management action plan is a document that sets out the strategy, structures, processes, activities and resources to appropriately manage the organization's risks to reduce or avoid adverse effects and grasp opportunities

☐ A plan that includes the strategy and rationale for addressing each category of risk with particular approaches

[Report Error](#)

Q. 12 Which of the following should be included as a critical starting-point when defining and developing the organization's GRC Strategic Plan? *

☐ Thresholds and tolerances

☐ System and processes

☒ Mission and vision

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Capability Strategic Plan is a document that details the structures, processes, technologies, resources, objectives, and measures to establish and maintain the capability needed to achieve the mission and vision.

☐ Fines and penalties

[Report Error](#)

Q. 13 Allocate GRC roles and responsibilities to individuals and committees with other roles while ensuring *

☒ Focus on objectives assigned to their primary roles

Explanation:- According to OCEG GRC Capability Model (Red Book) It is important to have Focus on objectives assigned to their primary roles

☐ Transparency of practices and activities

☐ Effectiveness of their control environment

☐ Required objectivity and independence

[Report Error](#)

Q. 14 All of the following are key management actions in the Assessment element EXCEPT: *

☒ Address inherently high risk

Explanation:- As per the OCEG GRC Capability Model (Red Book) Address inherently high risk is not key management action

☐ Analyze risk / reward

☐ Prioritize management of threats, opportunities and requirements

☐ Analyze compliance

[Report Error](#)

Q. 15 Which of the following is NOT a key management action in the Design element? *

☐ Explore options to address requirements

☐ Design transfer and risk financing strategies

☐ Develop key indicators

☒ Analyze risk / reward

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Analyze risk / reward belongs to A4 Assessment

[Report Error](#)

Q. 16 What category of risks are represented by financial fraud, operational fraud, corruption, and self-dealing? *

☐ Economic Risks

☐ Operational Risks

☐ Compliance Risks

☒ Integrity and Cultural Risks

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Reputation damage from issues such as poor product quality, employee misconduct, bribery, fraud, corruption, harassment, and intimidating behavior.

[Report Error](#)

Q. 17 Which best describes the steps to be taken when assessing risks and aligning management actions and controls to the organization's objectives? *

☒ Risk identification, risk analysis and determination of specific management actions and controls

Explanation:- According to OCEG GRC Capability Model (Red Book) The correct steps are - Risk identification, risk analysis and determination of specific management actions and controls

☐ Risk analysis, risk tactic selection and development of a risk mitigation plan

☐ Risk identification and risk categorization

☐ Risk categorization, risk management and development of risk indicators

[Report Error](#)

Q. 18 Which of the following is typically helpful for low likelihood and high impact risks that, should they materialize, would require financial resources beyond the organization's means? *

☐ Risk governance

☐ Risk optimization

☒ Risk financing

Explanation:- As per the OCEG GRC Capability Model (Red Book) SHARE the impact or optimization of the risk with other entities, including use of risk financing,

☐ Risk evaluation

[Report Error](#)

Q. 19 In the context of the GRC Capability Model, the word "promote" refers to which of the following? *

☐ Organizational risk management activities

☒ Desirable organizational conduct

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Policies both prohibit certain conduct and promote desired behavior while neither under-controlling nor over-controlling.

☐ Organizational GRC plan and activities

☐ Undesirable organizational events

[Report Error](#)

Q. 20 Which of the following is true regarding developing, implementing and managing policies? *

- ☒ Policies and procedures must be written to ensure that employees have guidelines for all decisions.

Explanation:- Option1: Policies and procedures must be written to ensure that employees have guidelines for all decisions. Explanation: Developing, implementing, and managing policies is an essential aspect of organizational governance. Policies provide guidance to employees about how to act in specific situations and ensure consistency in decision-making across the organization. Written policies are crucial to ensure that all employees are aware of the organization's expectations and can refer to them if they have any questions. The policies must be clear, concise, and understandable to ensure that employees can follow them without confusion. Option2: When writing policies, an organization cannot be too stringent in their effort to comply with laws and regulations - This option is incorrect because being too stringent in policy development can lead to unnecessary restrictions and hinder employee productivity. Option3: Although some policies will be informal in nature and do not have to be formally documented, employees will still be responsible to follow them - This option is incorrect because all policies must be documented and communicated to employees to ensure consistency and accountability. Option4: Having evidence that formal policies are communicated and enforced protects the organization when violations occur - This option is partly correct, but it only addresses the enforcement aspect of policy management. Policies must also be regularly reviewed and updated to ensure their continued relevance and effectiveness.

- ☐ When writing policies, an organization cannot be too stringent in their effort to comply with laws and regulations.

- ☐ Having evidence that formal policies are communicated and enforced protects the organization when violations occur.

< PREV

NEXT >

Q. 21 Which of the following is true regarding establishing proactive actions and controls to prevent and/or reduce the likelihood and/or impact of adverse events and misconduct? *

- ☐ Established procedures should go beyond those that are mandated, to include additional procedures that enable the organization to meet business objectives.
- ☐ The organization should design technology controls in a way that unauthorized human intervention is possible only by very high level managers who have had background checks.
- ☒ The organization should use physical controls to guard critical assets and to prevent any loss from occurring.

Explanation:- According to OCEG GRC Capability Model (Red Book) Establish proactive physical controls to meet mandated requirements, protect human health and safety. protect environmental conditions, and protect key physical assets and information assets.

- ☐ As long as formal policies are not required by law, related procedures do not have to be established.

[Report Error](#)

Q. 22 When conducting an internal review and investigation of allegations or indications of misconduct, management must *

- ☐ Make sure there are not too many channels of various types for reporting such incidents.
- ☒ Understand the facts, circumstances, root causes and appropriate resolution to such allegations or indications of misconduct.

Explanation:- As per the OCEG GRC Capability Model (Red Book) Establish an initial screening process to separate issues that can be quickly resolved from those that may need investigation.

- ☐ Ensure that the investigation does not interfere with any business operations of the organization.
- ☐ Immediately schedule external legal investigation to ensure independence in the review and investigation of the reported event.

[Report Error](#)

Q. 23 What is a GRC curriculum plan? *

- ☒ A plan setting out the order and timing of all courses for a particular role or family of roles, which may include a description of each course, its objectives, and method/mode of delivery

Explanation:- A GRC (Governance, Risk, and Compliance) curriculum plan is a plan setting out the order and timing of all courses for a particular role or family of roles related to GRC, which may include a description of each course, its objectives, and method/mode of delivery. Therefore, option is the correct answer. This plan helps to ensure that employees receive the appropriate GRC training to fulfill their job requirements and to maintain compliance with applicable laws and regulations.

- ☐ A plan describing what the organization intends to offer as training about GRC to the workforce, for approval by the board

- ☐ A plan setting out the names of all courses and training programs offered to the workforce by the organization

- ☐ A table of contents for the organization's training course about the GRC capability

Report Error

Q. 24 Which of the following is not an element in the Perform component? *

- ☐ Communication

- ☐ Inquiry

- ☐ Policies

- ☒ Assurance

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Assurance is not an element in the Perform component but of review

Report Error

Q. 25 Which of the following statements is NOT true? *

- ☒ Policies should only be established when required by law

Explanation:- According to OCEG GRC Capability Model (Red Book) Implement policies and associated procedures to address opportunities, threats and requirements and set clear expectations of conduct for the governing authority, management, the workforce and the extended enterprise.

- ☐ Adequate policy management includes being aware of all policies currently in place and confirming receipt or notification of them by target audiences
- ☐ Policies may both prohibit conduct and require conduct
- ☐ A documented policy development process can help to avoid the issuance of unauthorized policies

[Report Error](#)

Q. 26 When establishing procedures for investigating complaints or reports, an organization must *

- ☐ Define policies and procedures that ensure that such complaints or reports are never handled directly by line management.
- ☐ Define policies and procedures designed to make sure that the confidentiality of all reported information is protected.
- ☒ Define categories of issues that are significant enough to be escalated to senior management and/or outside counsel immediately upon validation.

Explanation:- As per the OCEG GRC Capability Model (Red Book) Establish an initial screening process to separate issues that can be quickly resolved from those that may need investigation.

- ☐ Define policies and procedures to ensure that the Board is aware of all compliance or ethical issues.

[Report Error](#)

Q. 27 With respect to third-party investigations and inquiries regarding allegations of misconduct, an organization must *

- ☐ Cooperate with external investigators by answering any requests.
- ☐ Be prepared to respond to all requests from external investigators as long as it is not suspected to lead to civil or criminal investigations.
- ☒ Be prepared to respond to a third-party investigation, while minimizing the business disruption of the investigation.

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Establish procedures to ensure that questions posed to the organization via a helpline or other method, that are identified as part of or precursor to a third party investigation are forwarded to appropriate personnel responsible for vetting such investigations.

- ☐ Not cooperate with the external investigation if they feel the investigation is frivolous.

[Report Error](#)

Q. 28 What are proactive actions and controls? *

- ☐ Technology and processes that help the organization to correct any detected instances of misconduct before an adverse impact arises
- ☐ Technology controls that detect the opportunity for misconduct or adverse events and prevent them from occurring
- ☒ Specified process steps or actions that will reduce the likelihood and impact of undesirable events, activities or behavior

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Proactive Actions & Controls proactively incentivize desirable and prevent undesirable conditions or events.

- ☐ Specified process steps or actions that will allow the organization to identify misconduct as it occurs

[Report Error](#)

Q. 29 What is a Policies and Procedures Matrix? *

- ☐ A list of policies including the procedures for implementing each policy
- ☐ A graph depicting each policy and procedure followed by each business unit
- ☐ A table indicating policies that are required by law mapped to each legal requirement
- ☒ A table correlating each policy to its owner, related requirements, related procedures, training, reports, controls and evidence of compliance

Explanation:- According to OCEG GRC Capability Model (Red Book) Policies and Related Procedures Matrix is a table correlating each policy to its attributes and other policies or procedures, and, optionally, to the training, reports, or other sources for evidence of compliance

[Report Error](#)

Q. 30 Which of the following is a mistake in the use of incentives? *

- ☐ Considering evidence of an individual's ethical conduct and consistency with organizational values in promotion decisions instead of training a newly promoted individual about ethical conduct
- ☐ Identifying ethical conduct as a factor in compensation decisions without including specific criteria and measures of conduct in performance reviews
- ☒ Using proactive controls in addition to human capital incentives such as bonuses and awards to gain the desired behavior

Explanation:- As per the OCEG GRC Capability Model (Red Book) The mistake is Using proactive controls in addition to human capital incentives such as bonuses and awards to gain the desired behavior as, proactive controls is present.

- ☐ Convincing employees that management views integrity and responsible conduct as values equal to obtaining strong financial performance

[Report Error](#)

Q. 31 Which of the following best describes effective proactive actions and controls of a GRC capability? *

- ☐ Providing a hotline for reporting of potential misconduct and flaws in the GRC capability which could lead to realization of adverse effects of risks
- ☐ Establishing a Code of Conduct, policies, training and a hotline for reporting about inappropriate conduct
- ☐ Establishing clear employee survey and exit interview procedures
- ☒ Promoting and motivating desired conduct while preventing undesirable events and activities through a mix of controls and incentives

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) To Establish Proactive Actions and Controls – Encourage desirable conditions, events, and conduct and prevent those that are undesirable

[Report Error](#)

Q. 32 Which of the following groups should be provided with repeated and consistent education about expected organizational conduct to increase the skills and motivation needed to help the organization achieve Principled Performance? *

- ☐ Organizational leaders, champions, and the extended enterprise
- ☐ Senior Management, the GRC capability support team, and the extended enterprise
- ☒ Organizational Board, senior management, workforce, and the extended enterprise

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Educate the governing authority, management, the workforce, and the extended enterprise about expected conduct, and increase the skills and motivation needed to help the organization address opportunities, threats, and requirements.

- ☐ Organizational learning and development team, and the extended enterprise

[Report Error](#)

Q. 33 Which one of the following enables individuals to know what is expected, to reduce the likelihood of errors, and to be comfortable about reporting misconduct or GRC capability flaws? *

☐ Code of conduct

☐ Detective actions and controls

☐ Policies

☒ Education

Explanation:- According to OCEG GRC Capability Model (Red Book) Education - Awareness, education, and ongoing support enables individuals to: Know what is expected, Reduce the likelihood of errors and criminal behavior, and Be comfortable about reporting misconduct or capability weaknesses

[Report Error](#)

Q. 34 Management implements various actions and controls to help ensure the organization meets its objectives, manages risks appropriately and is in compliance with applicable mandatory and voluntary boundaries. The OCEG Red Book version 3.0 discusses three specific categories of actions and controls. Which of the following is not a category of actions and controls described in the Red Book? *

☐ Proactive

☒ Mitigating

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Mitigating is not a category of actions and controls described in the Red Book

☐ Detective

☐ Responsive

[Report Error](#)

Q. 35 What is a common mistake when developing proactive technology controls? *

- ☐ Using detective controls at the same time as preventive controls
- ☐ Determining ways that a control may be circumvented or manipulated
- ☐ Using the same preventive technology control for more than one point of failure
- ☒ Allowing access to the technology control without evaluating role based need

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) For each process control activity: Define who will perform the activity

[Report Error](#)

Q. 36 Establishing a tiered approach for responding to investigations, helps with all of the following EXCEPT: *

- ☐ Ensure appropriate protection of anonymity and non-retaliation for reporters.
- ☐ Preserve records and other evidence.
- ☐ Capture and validate the incidents.
- ☒ Reducing the total impact to the organization from the event.

Explanation:- According to OCEG GRC Capability Model (Red Book) Reducing the total impact to the organization from the event does not help in establishing a tiered approach for responding to investigations

[Report Error](#)

Q. 37 Who should be informed of all notification pathways to report suspicions or incidents of noncompliance or unethical conduct and/or to identify concerns about GRC capability weaknesses? *

☒ Stakeholders and workforce

Explanation:- As per the OCEG GRC Capability Model (Red Book) Design the capability so stakeholders can trust, without fear of reprisal, that concerns are taken seriously, are promptly and objectively assessed and addressed, providing an option of anonymity where legally permitted or required. Implement a notification system that captures and alerts the organization to action and control weaknesses, performance variances, incidents or suspicions of legal noncompliance, violations of company policies, and concerns or perceptions about perceived unethical conduct.

☐ Board and compliance leaders

☐ Customers and business partners

☐ Senior management

[Report Error](#)

Q. 38 Which of the following is NOT a key management action and control related to Inquiry? *

☒ Adhere to data protection requirements

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Adhere to data protection requirements is NOT a key management action and control related to Inquiry

☐ Report information and findings.

☐ Establish multiple pathways to obtain information

☐ Establish and integrated approach to self-assessment.

[Report Error](#)

Q. 39 Which of the following are the three key management actions and controls described in the Notification element of the GRC Capability Model (Red Book)? *

- ☒ Capture notifications, filter and route notifications, and adhere to data protection requirements

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Capture notifications, filter and route notifications, and adhere to data protection requirements are the three key management actions and controls described in the Notification element of the GRC Capability Model (Red Book)

- ☐ Capture notifications, investigation, and remediation
- ☐ Detective controls, filter and route, and code of conduct
- ☐ Capture notifications, respond and resolve, and inform and integrate

[Report Error](#)

Q. 40 Which statement is FALSE? *

- ☐ The organization should conduct a needs assessment to determine training that will address high risk situations and develop a training plan for each job or job family
- ☐ 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
- ☐ The organization should have an awareness and education plan for each target population indicating what they should know about the GRC capability and their responsibilities for GRC activities
- ☒ Everyone in the organization should receive the same training and education about the GRC capability to ensure consistent understanding

Explanation:- According to OCEG GRC Capability Model (Red Book) Develop a job specific curriculum and appropriate training program for the governing authority, management, the workforce, and the extended enterprise to fulfill their responsibilities Same training and education about the GRC capability to ensure consistent understanding cannot be given to everyone in the organization

[Report Error](#)

Q. 41 Which of the following is NOT an appropriate step in the establishment of incentives? *

- ☒ Establish compensation plans for compliance oversight roles that include incentives tied to increased revenue

Explanation:- As per the OCEG GRC Capability Model (Red Book) Implement incentives that motivate desired conduct and recognize those who contribute to positive outcomes to reinforce desired conduct and not tied to revenue.

- ☐ Develop reward programs that recognize individuals for exhibiting desired conduct

- ☐ Designate rewards for units that demonstrate reduced compliance failures

- ☐ Avoid bonus incentives that encourage or reward misconduct

[Report Error](#)

Q. 42 Monitoring senior management's override of control activities is a responsibility requiring: *

- ☒ Board perspective and independence

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Board perspective and independence is needed to monitor senior management's override of control activities

- ☐ Investigation by the Chief Ethics Officer

- ☐ Review and correction by the Chief Legal Officer

- ☐ Reporting to senior management by the Chief Risk Officer

[Report Error](#)

Q. 43 When preparing to undertake an internal investigation related to compliance or ethical issues, an organization must *

- ☒ Define internal management that is responsible for oversight of the investigation.

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Develop internal investigation processes to address allegations or indications of undesirable conduct, and maintain a process for responding to external inquiries and investigations.

- ☐ Ensure the investigation does not interfere with any relevant business processes.
- ☐ Ensure that a completion due date for the investigation is set and adhered to in order that results are able to be reported on a timely basis.
- ☐ Immediately disclose the issue to the Board, independent auditors, or other applicable regulatory agencies.

[Report Error](#)

Q. 44 Which of these is a correct statement? *

- ☐ A code of conduct should be established only for management as required by law
- ☒ A code of conduct should address compliance with laws, conflicts of interest, use of corporate property, requirements and methods for reporting of misconduct, and other factors

Explanation:- According to OCEG GRC Capability Model (Red Book) Develop the code of conduct with the participation of stakeholders representing various levels of authority within the organization. Develop all codes of conduct required by legal or other mandates or one code that addresses all such requirements. Correlate the code of conduct to sources of requirements, principles, and values.

- ☐ A code of conduct always should specify that confidentiality will always be maintained for anyone reporting misconduct and provide a method for anonymous reporting
- ☐ A well written code of conduct may suffice to demonstrate that an organization has an effective compliance program

[Report Error](#)

Q. 45 A common mistake in setting up notification pathways is *

- ☒ Not capturing all notifications made via informal methods or unstructured channels.

Explanation:- As per the OCEG GRC Capability Model (Red Book) Capturing notifications made via informal methods, and unstructured channels, protects the organization from inconsistent management responses and provides better oversight into action and control weaknesses, noncompliance, and misconduct.

- ☐ Using technology resources as the pathway to provide notification.
- ☐ Encouraging stakeholders to raise concerns directly with the organization instead of going directly to external channels.
- ☐ Designing the capability so stakeholders can trust that concerns are taken seriously.

[Report Error](#)

Q. 46 Detective controls should *

- ☐ Establish mechanisms for identifying and analyzing risks
- ☐ Set the tone for the organization, influencing the control consciousness of its people
- ☒ Detect actual adverse events and indications of opportunity for any potential adverse events

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Detective Actions & Controls detect the actual or potential occurrence of desirable and undesirable conditions and events.

- ☐ Discourage errors or prevent irregularities from occurring

[Report Error](#)

Q. 47 Assurance on the effectiveness of the GRC capability should be performed by *

- ☐ The compliance function within the organization.
- ☐ The external auditor to ensure complete independence from the GRC capability.
- ☐ Control owners or those responsible for the various actions and controls.
- ☒ An independent, objective assurance function whether internal or external to the organization.

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) Independent, objective assurance personnel, using professional standards with experience in the subject matter, provide the highest level of assurance.

[Report Error](#)

Q. 48 One step in monitoring the GRC capability is monitoring and evaluating the capability design. This is performed by *

- ☐ Analyzing general risk associated with internal and external context to determine whether the risk level associated with the GRC capability is appropriate.
- ☐ Analyzing key areas in the internal and external context in which individuals might attempt to commit fraud.
- ☒ Re-evaluating the capability design in light of objectives, opportunities, threats, requirements, and changes to the context.

Explanation:- According to OCEG GRC Capability Model (Red Book) Appropriate monitoring methods for each aspect of the capability based on identified goals, assurance level and privilege status

- ☐ Analyzing key policies in the internal and external context that support the GRC capability.

[Report Error](#)

Q. 49 Which of the following statements is FALSE? *

- ☐ Assurance efforts are most effective when a risk based approach is used.
- ☒ Assurance should be performed by individuals who have the deepest understand of the actions and controls.

Explanation:- As per the OCEG GRC Capability Model (Red Book) Standards is focused, Independent, objective assurance personnel, using professional standards with experience in the subject matter, provide the highest level of assurance.

- ☐ Assurance desired may vary at different times and for different purposes.
- ☐ Assurance should focus on the ability of the GRC capability to meet its objectives while being consistent to the decision-making criteria.

[Report Error](#)

Q. 50 Which of the following is NOT a key assurance role responsibility with regard to the GRC capability? *

- ☐ Determining that risks and requirements are correctly identified, evaluated, managed and monitored
- ☒ Maintaining the operation of established controls

Explanation:- With reference to the OCEG GRC Capability Model (Red Book) Maintaining the operation of established control is not a key assurance role responsibility with regard to the GRC capability but only Plan and perform Assurance Assessment are included as rest options.

- ☐ Assessing the design of the GRC capability to provide assurance of its ability to address identified risks and requirements
- ☐ Ensuring that the board or other oversight authorities have quality information on which to make decisions about the GRC capability

[Report Error](#)

Q. 51 When developing a GRC technology architecture, an organization should *

- ☐ Ensure that all processes are automated to reduce the risk of employee error.
- ☐ Ensure that the GRC technology plan is developed and maintained separately from the overall IT technology plan to avoid any conflict of interest.
- ☒ Enable the GRC capability with a technology architecture that integrates with and, where appropriate, uses existing investments in technology.

Explanation:- Referring to the OCEG GRC Capability Model (Red Book) To develop technology architecture: Identify key processes controls that are less error-prone and more efficient if enabled by technology, Understand existing technology environment, Map functionality requirements to existing capabilities and Identify redundancies in existing technology solutions.

- ☐ Ensure that employees responsible for GRC activities develop a detailed plan for their GRC technology architecture so they are able to present this plan to the IT Department for implementation.

Report Error

Q. 52 What is an important principle to keep in mind when establishing an approach to embedding the GRC capability into the business? *

- ☐ Legal mandates for independence will not preclude combining certain responsibilities into one role if the specific individual in the role can demonstrate independence and appropriate decision making
- ☒ Irreconcilable conflicts of interest or legal mandates may preclude combining certain responsibilities under one role

Explanation:- According to OCEG GRC Capability Model (Red Book) Define job/role descriptions for all key roles, including designation of which duties are segregated to prevent conflicts of interest.

- ☐ Responsibilities combined into one role will not require any controls to ensure objectivity and independence if there is no legal mandate requiring segregation of duties
- ☐ Conflicts of interest will not preclude combining certain responsibilities into one role if training is provided to the individual in that role

Report Error