OCEG

GRCA Exam

GRC Auditor Certification Exam

Questions & Answers
Demo

Version: 4.0

Question: 1

Which of the following is defined as "a measure of the desirable effect of uncertainty on objectives?

A. Risk
B. Compliance
C. Reward

Answer: A

Explanation:
Risk is defined as a measure of the desirable effect of uncertainty on objectives. According to the ISO 31000 standard, risk is "the effect of uncertainty on objectives" which can be either positive (opportunity) or negative (threat). This definition encompasses the uncertainty that can impact the achievement of goals and objectives. It highlights that risk is not just about potential losses but also about potential gains that come from taking risks.
Reference:
ISO 31000:2018 - Risk management – Guidelines
NIST SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments

Question: 2

The two kinds of PROACTIVE controls are

A. training and education
B. promoting and preventive
C. access and system

Answer: B

Explanation:
Proactive controls are those measures implemented to prevent undesirable events before they occur. Promoting controls are designed to encourage desired behaviors and outcomes, such as compliance with policies and procedures. Preventive controls are aimed at stopping undesirable events or actions before they happen, such as implementing security measures to prevent unauthorized access. Both types of controls are essential for effective risk management and ensuring the security and integrity of an organization's processes and systems.
Reference:
COSO Internal Control – Integrated Framework

ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls

Question: 3

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

A. Governance
B. Assurance
C. Management

Answer: A

Explanation:
Governance is defined as "externally directing, controlling and evaluating an entity, process, or resource". It involves establishing policies, and continuous monitoring of their proper implementation, by the members of the governing body of an organization. It ensures that the entity is operating effectively and in alignment with its objectives and regulatory requirements. Governance encompasses a wide range of activities, including strategic planning, decision-making, and oversight, all aimed at achieving the entity's goals while managing risk and ensuring compliance.
Reference:
ISO 38500:2015 - Information technology - Governance of IT for the organization
OECD Principles of Corporate Governance

Question: 4

Producing Value and Protecting Value are trade-offs. You CANNOT do both at the same time. *

A. True
B. False

Answer: B

Explanation:
The statement that producing value and protecting value are trade-offs and cannot be done at the same time is false. In fact, both can and should be pursued concurrently. Effective governance, risk management, and compliance (GRC) strategies integrate the production of value (achieving business objectives and growth) with the protection of value (safeguarding assets, ensuring compliance, and managing risks). This integrated approach ensures sustainable performance and long-term success. Organizations that balance both aspects can achieve principled performance by reliably achieving objectives, addressing uncertainty, and acting with integrity.
Reference:
ISO 31000:2018 - Risk management – Guidelines
COSO Enterprise Risk Management – Integrating with Strategy and Performance

Question: 5

Which of the following is defined as "a measure of the degree to which obligations and requirements are addressed"

A. Risk
B. Compliance
C. Reward

Answer: B

Explanation:
Compliance is defined as a measure of the degree to which obligations and requirements are addressed. It involves adhering to laws, regulations, policies, and standards that are relevant to the organization. Compliance ensures that the organization meets its legal and ethical obligations, thereby avoiding legal penalties, reputational damage, and operational disruptions. Effective compliance programs involve continuous monitoring, training, and auditing to ensure all requirements are met and maintained.
Reference:
ISO 19600:2014 - Compliance management systems - Guidelines
NIST SP 800-37 Rev. 2 - Risk Management Framework for Information Systems and Organizations