Download Isaca NIST-COBIT-2019 Exam Dumps Free

Shared by Good on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An organization is concerned that there will be resistance in attempts to close gaps between the current and target profiles. Which of the following is the

BEST approach to gain support for the process?

Options:

A- Implement organization-wide training on the CSF.
B- Communicate management opinions regarding the project.
C- Identify quick wins for implementation first.

Answer:

C

Explanation:

Identifying quick wins for implementation first is the best approach to gain support for the process, as it can demonstrate the value and feasibility of the project, and motivate the stakeholders to overcome the resistance and embrace the change12. Quick wins are those actions that can be implemented rapidly and easily, and that can produce visible and measurable results3.

Reference 7 Phases in COBIT Implementation | COBIT Certification - Simplilearn Implementing the NIST Cybersecurity Framework Using COBIT 2019, page 17. What is a Quick Win? - Definition from Techopedia

Question 2

Question Type: MultipleChoice

Which of the following is a framework principle established by NIST as an initial framework consideration?

Options:

A- Avoiding business risks
B- Impact on global operations
C- Ensuring regulatory compliance

Answer:

C

Explanation:

One of the framework principles established by NIST is to ensure that the framework is consistent and aligned with existing regulatory and legal requirements that are relevant to cybersecurity12.

Question 3

Question Type: MultipleChoice

Which role will benefit MOST from a better understanding of the current cybersecurity posture by applying the CSF?

Options:

A- Executives
B- Acquisition specialists
C- Legal experts

Answer:

A

Explanation:

Executives are the role that will benefit most from a better understanding of the current cybersecurity posture by applying the CSF. This is because executives are responsible for setting the strategic direction, objectives, and priorities for the organization, as well as overseeing the allocation of resources and the management of risks1. By applying the CSF, executives can gain a comprehensive and consistent view of the cybersecurity risks and capabilities of the organization, and align them with the business goals and requirements2. The CSF can also help executives communicate and collaborate with other stakeholders, such as regulators, customers, suppliers, and partners, on cybersecurity issues3.

Question 4

Question Type: MultipleChoice

Within the CSF Core structure, which type of capability can be implemented to help practitioners recognize potential or realized risk to enterprise assets?

Options:

A- Protection capability
B- Response capability
C- Detection capability

Answer:

C

Explanation:

The Detection capability is the type of capability within the CSF Core structure that can help practitioners recognize potential or realized risk to enterprise assets. The Detection capability consists of six categories that enable timely discovery of cybersecurity events, such as Anomalies and Events, Security Continuous Monitoring, and Detection Processes12.

Question 5

Question Type: MultipleChoice

Which CSF step corresponds to the COBIT objective of knowledge and understanding of enterprise goals?

Options:

A- Step 1: Prioritize and Scope
B- Step 6: Determine, Analyze, and Prioritize Gaps
C- Step 4: Conduct a Risk Assessment

Answer:

A

Explanation:

This CSF step corresponds to the COBIT objective of knowledge and understanding of enterprise goals, because it involves identifying the business drivers, mission, objectives, and risk appetite of the organization, as well as the scope and boundaries of the cybersecurity program12. This step helps to ensure that the cybersecurity activities and outcomes are aligned with the enterprise goals and strategy34.

Question 6

Question Type: MultipleChoice

Which information should be collected for a Current Profile?

Options:

A- Implementation Status
B- Recommended Actions
C- Resource Required

Answer:

A

Explanation:

The implementation status is the information that should be collected for a Current Profile, because it indicates the degree to which the cybersecurity outcomes defined by the CSF Subcategories are currently being achieved by the organization12. The implementation status can be expressed using a four-level scale: Not Performed, Partially Performed, Performed, and Informative Reference Not Applicable34.

Question 7

Question Type: MultipleChoice

In which CSF step should an enterprise document its existing category and subcategory outcome achievements?

Options:

A- Step 1: Prioritize and Scope
B- Step 3: Create a Current Profile
C- Step 4: Conduct a Risk Assessment

Answer:

B

Explanation:

This CSF step involves documenting the existing category and subcategory outcome achievements, by using the implementation status to indicate the degree to which the cybersecurity outcomes defined by the CSF Subcategories are currently being achieved by the organization12. The Current Profile reflects the current cybersecurity posture of the organization, and helps to identify the gaps and opportunities for improvement3 .

Question 8

Question Type: MultipleChoice

When aligning to the NIST Cybersecurity Framework, what should occur after tier levels and framework core outcomes are determined?

Options:

A- Report discovered issues to senior management.
B- Assign mitigating control development.
C- Compare current and target profiles.

Answer:

C

Explanation:

According to the NIST Cybersecurity Framework, after determining the tier levels and framework core outcomes, the next step is to compare the current and target profiles, which describe the organization's current and desired cybersecurity posture based on the framework core functions, categories, and subcategories1. This comparison helps to identify the gaps and prioritize the actions for improvement2.

Reference Cybersecurity Framework Components | NIST What is the NIST Cybersecurity Framework? | IBM