ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

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

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.
Reference: 1: Cybersecurity Framework | NIST 2: Framework Documents | NIST

Question: 2

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

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.
Reference: 1: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 2: Cybersecurity Framework | NIST 3: Framework Documents | NIST

Question: 3

When coordinating framework implementation, the business/process level collaborates with the implementation/operations level to:

A. develop the risk management framework.
B. assess changes in current and future risks.
C. create the framework profile.

Answer: B

Explanation:

According to the TM Forum's Business Process Framework (eTOM), the business/process level is responsible for defining the business strategy, objectives, and requirements, as well as monitoring and controlling the performance and quality of the processes1. The implementation/operations level is responsible for designing, developing, and executing the processes that deliver and support the services1. When coordinating framework implementation, these two levels collaborate to assess changes in current and future risks, such as market trends, customer expectations, regulatory compliance, security threats, and operational issues2. This helps them to align the processes with the business goals and outcomes, and to identify and mitigate any potential gaps or challenges3. Reference: 1: Process Framework (eTOM) - TM Forum 2: Implement Dynamics 365 with a process- focused approach 3: Operations Management Implementation - Smarter Solutions, Inc.

Question: 4

Which of the following COBIT 2019 governance principles corresponds to the CSF application stating that CSF profiles support flexibility in content and structure?

A. A governance system should be customized to the enterprise needs, using a set of design factors as parameters.
B. A governance system should focus primarily on the enterprise's IT function and information processing.
C. A governance system should clearly distinguish between governance and management activities and structures.

Answer: A

Explanation:

This principle corresponds to the CSF application stating that CSF profiles support flexibility in content and structure, because both emphasize the need for tailoring the governance system to the specific context and requirements of the enterprise12. The CSF profiles are based on the enterprise's business drivers, risk appetite, and current and target cybersecurity posture3. The COBIT 2019 design factors are a set of parameters that influence the design and operation of the governance system, such as enterprise strategy, size, culture, and regulatory environment4.

Reference: 1: COBIT | Control Objectives for Information Technologies | ISACA 2: COBIT 2019 Framework – ITSM Docs - ITSM Documents & Templates 3: Framework Documents | NIST 4: Introduction to COBIT Principles - Testprep Training Tutorials

Question: 5

Which of the following functions provides foundational activities for the effective use of the Cybersecurity Framework?

A. Protect
B. Identify
C. Detect

Answer: B

Explanation:

The Identify function provides foundational activities for the effective use of the Cybersecurity Framework, because it assists in developing an organizational understanding of managing cybersecurity risk to systems, people, assets, data, and capabilities12. This understanding enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs12. The Identify function includes outcome categories such as Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management12.
Reference: 1: The Five Functions | NIST 2: Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide

Question: 6

What does a CSF Informative Reference within the CSF Core provide?

A. A high-level strategic view of the life cycle of an organization's management of cybersecurity risk
B. A group of cybersecurity outcomes tied to programmatic needs and particular activities
C. Specific sections of standards, guidelines, and practices that illustrate a method to achieve an associated outcome

Answer: C

Explanation:

A CSF Informative Reference within the CSF Core provides a citation to a related activity from another standard or guideline that can help an organization achieve the outcome described in a CSF Subcategory12. For example, the Informative Reference for ID.AM-1 (Physical devices and systems within the organization are inventoried) is COBIT 5 APO01.01, which states "Maintain an inventory of IT assets"3.
Reference: 1: Informative Reference: What are they, and how are they used? | NIST 2: Everything to Know About NIST CSF Informative Reference | Axio 3: NIST Cybersecurity Framework v1.1 - CSF Tools - Identity Digital

Question: 7

Analysis is one of the categories within which of the following Core Functions?

A. Detect
B. Respond
C. Recover

Answer: A

Explanation:

Analysis is one of the six categories within the Detect function of the NIST Cybersecurity Framework. The Analysis category aims to identify the occurrence of a cybersecurity event by performing data aggregation, correlation, and analysis12.
Reference: 1: The Five Functions | NIST 2: Cybersecurity Framework Components | NIST

Question: 8

Which of the following is associated with the "Detect" core function of the NIST Cybersecurity Framework?

A. Information Protection Processes and Procedures
B. Anomalies and Events
C. Risk Assessment

Answer: B

Explanation:
Anomalies and Events is one of the six categories within the Detect function of the NIST Cybersecurity Framework. The Anomalies and Events category aims to ensure that anomalous activity is detected in a timely manner and the potential impact of events is understood12.
Reference: 1: The Five Functions | NIST 2: Detect | NIST

Question: 9

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

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.
Reference: 1: The Five Functions | NIST 2: Cybersecurity Framework | NIST

Question: 10

The CSF Implementation Tiers distinguish three fundamental dimensions of risk management to help

enterprises evaluate which of the following?

A. Cybersecurity posture
B. Cybersecurity threats
C. Cybersecurity landscape

Answer: A

Explanation:

The CSF Implementation Tiers distinguish three fundamental dimensions of risk management to help enterprises evaluate their cybersecurity posture, which is the alignment of their cybersecurity activities and outcomes with their business objectives and risk appetite12. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe the degree of rigor, integration, and collaboration of the organization's cybersecurity risk management practices12.

Reference: 1: Cybersecurity Framework Components | NIST 2: Cybersecurity Framework FAQs Framework Components | NIST

Question: 11

What is the MOST important reason to compare framework profiles?

A. To improve security posture
B. To conduct a risk assessment
C. To identify gaps

Answer: C

Explanation:

The most important reason to compare framework profiles is to identify gaps between the current and target state of cybersecurity activities and outcomes, and to prioritize the actions needed to address them12. Framework profiles are the alignment of the functions, categories, and subcategories of the NIST Cybersecurity Framework with the business requirements, risk tolerance, and resources of the organization3. By comparing the current profile (what is being achieved) and

the target profile (what is needed), an organization can assess its cybersecurity posture and develop a roadmap for improvement4.

Reference: 1: Cybersecurity Framework Components | NIST 2: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 3: Examples of Framework Profiles | NIST 4: Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA

Question: 12

The goals cascade supports prioritization of management objectives based on:

A. the prioritization of enterprise goals.
B. the prioritization of business objectives.

C. the prioritization of stakeholder needs.

Answer: C

Explanation:

The goals cascade is a mechanism that translates the stakeholder needs into specific, actionable, and customized goals at different levels of the enterprise12. The stakeholder needs are the drivers of the governance system and reflect the expectations and requirements of the internal and external parties that have an interest or influence on the enterprise34. The goals cascade supports the prioritization of management objectives based on the stakeholder needs, as well as the alignment of the enterprise goals, the alignment goals, and the governance and management objectives12. Reference: 1: COBIT 2019 Goals Cascade: A Blueprint for Success 2: COBIT 2019 Framework – ITSM Docs - ITSM Documents & Templates 3: COBIT | Control Objectives for Information Technologies | ISACA 4: Aligning IT goals using the COBIT5 Goals Cascade

Question: 13

The seven high-level CSF steps generally align to which of the following in COBIT 2019?

A. High-level phases
B. High-level functions
C. High-level categories

Answer: A

Explanation:

The seven high-level CSF steps generally align to the high-level phases of the COBIT 2019 implementation guide, which are: What are the drivers?; Where are we now?; Where do we want to be?; What needs to be done?; How do we get there?; Did we get there?; and How do we keep the momentum going?12. These phases provide a structured approach for implementing a governance system using COBIT 2019, and can be mapped to the CSF steps of Prioritize and Scope, Orient, Create a Current Profile, Conduct a Risk Assessment, Create a Target Profile, Determine, Analyze and Prioritize Gaps, and Implement Action Plan34.
Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3:

Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 4: REVIEW OF IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK USING COBIT 2019.

Question: 14

Which of the following is the MOST important input for prioritizing resources during program initiation?

A. Replacement cost
B. Risk register
C. Business impact assessment

Answer: C

Explanation:

A business impact assessment (BIA) is the most important input for prioritizing resources during program initiation, because it helps to identify and evaluate the potential effects of disruptions to critical business functions and processes12. A BIA can help to determine the recovery objectives, priorities, and strategies for the program, as well as the resource requirements and dependencies34. Reference: 1: Business Impact Analysis | Ready.gov 2: Business Impact Analysis - ISACA 3: COBIT 2019 Implementation Guide 4: COBIT 2019 Implementation - ISACA

Question: 15

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

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.
Reference: 1: Cybersecurity Framework Components | NIST 2: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 3: COBIT 2019 Design and Implementation COBIT Implementation5 4: COBIT® 2019 Foundation | Skillsoft Global Knowledge6

Question: 16

Which of the following COBIT tasks and activities corresponds to CSF Step 1: Prioritize and Scope?

A. Understand the enterprise's capacity and capability for change.
B. Use change agents to communicate informally and formally.
C. Determine ability to implement the change.

Answer: A

Explanation:

This COBIT task and activity corresponds to CSF Step 1: Prioritize and Scope, because it involves assessing the current state of the enterprise’s governance and management system, as well as its readiness and ability to adopt changes12. This task and activity is part of the COBIT 2019 implementation phase "Where are we now?"3, which aligns with the CSF step of identifying the business drivers, mission, objectives, and risk

appetite of the organization4.
Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3: Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA 4: Cybersecurity Framework Components | NIST

Question: 17

Which of the following is an input to COBIT Implementation Phase 1: What Are the Drivers?

A. Risk response document
B. Current capability rating for selected processes
C. Program wake-up call

Answer: C

Explanation:

A program wake-up call is an input to COBIT Implementation Phase 1: What Are the Drivers, because it is a trigger event that creates a sense of urgency and a need for change in the organization's governance and management of enterprise I&T12. A program wake-up call can be internal or external, positive or negative, such as a major incident, a new regulation, a strategic initiative, or a stakeholder feedback34.
Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3: Tips for Implementing COBIT in a Continuously Changing Environment - ISACA 4: 7 Phases of COBIT Implementation: Explained - The Knowledge Academy

Question: 18

Which information should be collected for a Current Profile?

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.
Reference: 1: Cybersecurity Framework Components | NIST 2: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 3: Framework Documents | NIST 4: REVIEW OF IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK USING COBIT 2019.

Question: 19

During Step 3: Create a Current Profile, an enterprise outcome has reached a 95% subcategory maturity level. How would this level of achievement be described in the COBIT Performance Management

Rating Scale?

A. Largely Achieved
B. Partially Achieved
C. Fully Achieved

Answer: C

Explanation:

According to the COBIT Performance Management Rating Scale, a subcategory maturity level of 95% corresponds to the rating of Fully Achieved, which means that the outcome is achieved above 85%12. This indicates that the enterprise has a high degree of capability and maturity in the subcategory, and that the practices and activities are performed consistently and effectively34.
Reference: 1: Performance Management of Processes - Testprep Training Tutorials 2: COBIT 2019 and COBIT 5 Comparison - ISACA 3: COBIT 2019 Performance Management: Principles and Processes 4: Effective Capability and Maturity Assessment Using COBIT 2019 - ISACA

Question: 20

During CSF implementation, when is an information security manager MOST likely to identify key enterprise and supporting alignment goals as previously understood?

A. CSF Steps 5: Create a Target Profile and 6: Determine, Analyze, and Prioritize Gaps
B. CSF Step 1: Prioritize and Scope
C. CSF Steps 2: Orient and 3: Create a Current Profile

Answer: B

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.
Reference: 1: Cybersecurity Framework Components | NIST 2: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 3: COBIT 2019 Design and Implementation COBIT Implementation 4: COBIT® 2019 Foundation | Skillsoft Global Knowledge

Question: 21

During the implementation of Step 2: Orient and Step 3: Create a Current Profile, the organization's asset register should primarily align to:

A. organizational strategy.
B. configuration management.
C. the security business case.

Answer: B

Explanation:

The organization's asset register should primarily align to configuration management, because it is a process that maintains an accurate and complete inventory of the organization's I&T assets and their relationships12. Configuration management supports the implementation of Step 2: Orient and Step 3: Create a Current Profile, because it helps to identify the systems, people, assets, data, and capabilities that are within the scope of the cybersecurity program, and to assess their current cybersecurity outcomes34.
Reference: 1: COBIT 2019 Framework – ITSM Docs - ITSM Documents & Templates 2: COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution 3: Cybersecurity Framework Components | NIST 4: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA

Question: 22

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

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 .
Reference: 1: Cybersecurity Framework Components | NIST 2: Cybersecurity Framework v1.1 - CSF Tools - Identity Digital 3: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA : REVIEW OF IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK USING COBIT 2019.

Question: 23

Which of the following represents a best practice for completing CSF Step 3: Create a Current Profile?

A. Procuring solutions that are cost-effective and fit the organization's technical architecture
B. Assessing current availability, performance, and capacity to create a baseline
C. Engaging in a dialogue and obtaining input to determine appropriate goals, tiers, and Activities

Answer: C

Explanation:

This represents a best practice for completing CSF Step 3: Create a Current Profile, because it involves collaborating with relevant stakeholders to identify the current cybersecurity outcomes and implementation status of the organization12. Engaging in a dialogue and obtaining input can help to ensure that the Current Profile reflects the business drivers, mission, objectives, and risk appetite of the organization, as well as the scope and boundaries of the cybersecurity program34.
Reference: 1: Cybersecurity Framework Components | NIST 2: Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide3 3: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 4: NIST CSF: The seven-step cybersecurity framework process5

Question: 24

Identifying external compliance requirements is MOST likely to occur during which of the following COBIT implementation phases?

A. Phase 4 - What Needs to Be Done?
B. Phase 2 - Where Are We Now?
C. Phase 3 - Where Do We Want to Be?

Answer: B

Explanation:
Identifying external compliance requirements is most likely to occur during COBIT Implementation Phase 2: Where Are We Now?, because this phase involves assessing the current state of the enterprise's governance and management system, as well as its strengths, weaknesses, opportunities, and threats12. This phase also includes identifying the relevant stakeholders, drivers,

and scope of the implementation program . Therefore, this phase requires a thorough understanding of the external laws, regulations, and contractual obligations that apply to the enterprise and its I&T activities.
Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA : Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA : 7 Phases of COBIT Implementation: Explained - The Knowledge Academy : Compliance with External Requirements - Morland-Austin

Question: 25

Which of the following is a PRIMARY input into Steps 2 and 3: Orient and Create a Current Profile?

A. Evaluating business cases
B. Updating business cases
C. Defining business cases

Answer: C

Explanation:

Defining business cases is a primary input into Steps 2 and 3: Orient and Create a Current Profile, 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. A business case is a document that provides the

rationale and justification for initiating a cybersecurity project or program, and describes the expected benefits, costs, risks, and alternatives34.

Reference: 1: Cybersecurity Framework Components | NIST 2: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 3: Business Case Development - ISACA 4: How to Write a Business Case for Cybersecurity Projects | Infosec

Question: 26

Which of the following is a KEY activity of COBIT Implementation Phase 2: Where Are We Now?

A. Identification of applicable compliance requirements
B. Identification of challenges and success factors
C. Identification and definition of improvement targets

Answer: A

Explanation:

This is a key activity of COBIT Implementation Phase 2: Where Are We Now?, because it involves assessing the current state of the enterprise's governance and management system, as well as its strengths, weaknesses, opportunities, and threats12. This activity also includes identifying the relevant stakeholders, drivers, and scope of the implementation program. Therefore, this activity requires a thorough understanding of the external laws, regulations, and contractual obligations that apply to the enterprise and its I&T activities34.

Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3: Compliance with External Requirements - Morland-Austin 4: COBIT 5 : Key Concepts and Principles of COBIT 5 Explained

Question: 27

Which of the following is an objective of COBIT Implementation Phase 3-Where Do We Want to Be?

A. Identify critical processes or other components addressed in the improvement plan.
B. Determine the target capability for processes within governance and management
C. objectives.
D. Integrate the metrics for project performance and benefits realization.

Answer: B

Explanation:

This is an objective of COBIT Implementation Phase 3: Where Do We Want to Be?, because it involves defining the desired state of the enterprise's governance and management system, based on the stakeholder needs, drivers, and scope12. This objective also includes using the COBIT Performance Management system to assess the current and target capability levels of the processes that support the governance and management objectives34.

Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3: COBIT 2019 Performance Management: Principles and Processes 4: Effective Capability and Maturity Assessment Using COBIT 2019 - ISACA

Question: 28

Which of the following is an objective of Implementation Phase 3 - Where Do We Want to Be?

A. Integrate the improvement projects into the overall program plan.
B. Monitor, measure, and report on project progress.
C. Create a detailed business case and high-level program plan from gathered information.

Answer: C

Explanation:

This is an objective of Implementation Phase 3: Where Do We Want to Be?, because it involves defining the desired state of the enterprise's governance and management system, based on the stakeholder needs, drivers, and scope12. This objective also includes developing a business case that provides the rationale and justification for the improvement program, and a high-level program plan that outlines the scope, objectives, approach, and resources of the program3 .

Reference: 1: COBIT 2019 Implementation Guide 2: COBIT 2019 Implementation - ISACA 3: Business Case Development - ISACA : How to Write a Business Case for Cybersecurity Projects | Infosec

Question: 29

Which of the following is an objective of COBIT Implementation Phase 3 - Where Do We Want to Be?

A. Determine the current capability of selected processes.
B. Identify critical processes or other components addressed in the improvement plan.
C. Create a detailed business case and high-level program plan.

Answer: C

Explanation:

The objective of COBIT Implementation Phase 3 is to set an improvement target and identify gaps and potential solutions using COBIT's guidance. This involves creating a detailed business case and a high-level program plan for the implementation.

Reference

COBIT 2019 Design and Implementation COBIT Implementation, page 31.

7 Phases in COBIT Implementation | COBIT Certification - Simplilearn

Question: 30

Documenting opportunities for improvement occurs within which implementation phase?

A. Phase 4 - What Needs to Be Done?

B. Phase 2 - Where Are We Now?
C. Phase 3 - Where Do We Want to Be?

Answer: B

Explanation:

The objective of COBIT Implementation Phase 2 is to define the scope of the implementation using COBIT's mapping of enterprise goals to IT-related goals and the associated IT processes, and to consider how risk scenarios could also highlight key processes on which to focus. This phase also involves documenting the current capability and performance of the selected processes and identifying opportunities for improvement12.

Reference

7 Phases in COBIT Implementation | COBIT Certification - Simplilearn COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 31

Which of the following COBIT and NIST implementation steps may be reversed depending on the culture of the organization?

A. Step 4: Conduct a Risk Assessment and Step 6: Determine, Analyze, and Prioritize Gaps
B. Step 3: Create a Current Profile and Step 5: Create a Target Profile
C. Step 1: Prioritize and Scope and Step 2: Orient

Answer: C

Explanation:

According to the ISACA guide, the order of these two steps may be reversed depending on the culture of the organization and the level of stakeholder engagement1. Some organizations may prefer to start with a broad orientation of the NIST CSF and COBIT 2019 before scoping and prioritizing the implementation, while others may want to define the scope and priorities first and then orient the stakeholders accordingly.

Reference

Implementing the NIST Cybersecurity Framework Using COBIT 2019, page 17.

Question: 32

Which of the following is the MOST critical process tool to performing Implementation Phase 3- Where Do We Want to Be?

A. Control self-assessment
B. Gap assessment
C. Cost-benefit analysis

Answer: B

Explanation:

A gap assessment is the most critical process tool to performing Implementation Phase 3, as it helps to identify the current and desired states of the selected processes, and the gaps and potential solutions to bridge them. A gap assessment also helps to create a detailed business case and a high- level program plan for the implementation12.

Reference

7 Phases in COBIT Implementation | COBIT Certification - Simplilearn

COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 33

The activity of determining an appropriate target capability level for each process occurs within which implementation phase?

A. Phase 4 - What Needs to Be Done?
B. Phase 3 - Where Do We Want to Be?
C. Phase 2 - Where Are We Now?

Answer: B

Explanation:

The activity of determining an appropriate target capability level for each process occurs within Implementation Phase 3, as it helps to set an improvement target and identify gaps and potential solutions using COBIT's guidance. This involves creating a detailed business case and a high-level program plan for the implementation12.

Reference

Defining Target Capability Levels in COBIT 2019: A Proposal for Refinement

COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 34

Which of the following should an organization review to gain a better understanding of the likelihood and impact of cybersecurity events?

A. Relevant internal or external capability benchmarks
B. Cybersecurity frameworks, standards, and guidelines
C. Cyber threat information from internal and external sources

Answer: C

Explanation:

According to the NIST Cybersecurity Framework, an organization should review cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events. This information can help the organization to identify potential threats, vulnerabilities, and consequences, and to assess the current and target profiles of its cybersecurity posture12.

Reference

Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management, page 19.

COBIT VS NIST : A Comprehensive Analysis - ITSM Docs

Question: 35

Which of the following is an important consideration when defining the roadmap in COBIT Implementation Phase 3 - Where Do We Want to Be?

A. Agreed metrics for measuring outcomes
B. Reporting procedures and requirements
C. Change-enablement implications

Answer: C

Explanation:

An important consideration when defining the roadmap in COBIT Implementation Phase 3 is the change-enablement implications, which refer to the potential impact of the proposed solutions on the people, culture, and behavior of the organization. This involves assessing the readiness and willingness of the stakeholders to adopt the changes, identifying the risks and barriers to change, and developing strategies to address them12.

Reference

7 Phases in COBIT Implementation | COBIT Certification - Simplilearn COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 36

Which of the following is MOST important for successful execution of CSF implementation Step 6 - Determine, Analyze, and Prioritize Gaps?

A. Have management review and approve the gap analysis.
B. Engage external experts to perform a cost-benefit analysis.
C. Engage business and IT process owners for internal expertise.

Answer: C

Explanation:

According to the ISACA guide, engaging business and IT process owners for internal expertise is most important for successful execution of CSF implementation Step 6, as they can provide valuable insights into the current and desired states of the processes, the gaps and potential solutions, and the costs and benefits of the implementation1. They can also help to align the cybersecurity program with the business objectives

and risk appetite of the organization. Reference
Implementing the NIST Cybersecurity Framework Using COBIT 2019, page 17.

Question: 37

How should gaps identified between the current and target profiles be addressed?

A. Comparing to and acting on the desired Tier level
B. With a full project engagement to close all gaps
C. Through a risk based-approach

Answer: C

Explanation:
According to the NIST Cybersecurity Framework, gaps identified between the current and target profiles should be addressed through a risk-based approach, which enables an organization to gauge the resources needed and prioritize the mitigation of gaps in a cost-effective manner. This approach also aligns the cybersecurity program with the business objectives and risk appetite of the organization12.
Reference
Examples of Framework Profiles | NIST
What is the NIST Cybersecurity Framework? | IBM

Question: 38

When aligning to the NIST Cybersecurity Framework, what should occur after tier levels and

framework core outcomes are determined?

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

Question: 39

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?

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: 40

Which of the following should be a PRIMARY consideration when creating an action plan to address gaps identified in CSF Step 6: Determine, Analyze, and Prioritize Gaps?

A. Mission drivers
B. Stakeholder map
C. IT process descriptions

Answer: A

Explanation:

According to the NIST Cybersecurity Framework, mission drivers are a primary consideration when creating an action plan to address gaps identified in CSF Step 6, as they help to align the cybersecurity program with the organization's objectives, priorities, and risk appetite. Mission drivers also help to determine the resources needed and the cost-benefit analysis of the proposed solutions12.

Reference

7 Steps to Implement & Improve Cybersecurity with NIST

Cybersecurity Framework v1.1 - CSF Tools - Identity Digital, page 7.

Question: 41

Which COBIT implementation phase directs the development of an action plan based on the outcomes described in the Target Profile?

A. Phase 3 -Where Do We Want to Be?
B. Phase 5 -How Do We Get There?

C. Phase 4 -What Needs to Be Done?

Answer: B

Explanation:
The COBIT implementation phase that directs the development of an action plan based on the outcomes described in the Target Profile is Phase 5 - How Do We Get There? This phase involves defining the detailed steps, resources, roles, and responsibilities for executing the implementation plan and achieving the desired outcomes12.

Reference
7 Phases in COBIT Implementation | COBIT Certification - Simplilearn COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 42

Which of the following is one of the objectives of CSF Step 6: Determine, Analyze and Prioritize Gaps?

A. Translate improvement opportunities into justifiable, contributing projects.
B. Direct stakeholder engagement, communication, and reporting.
C. Communicate the I&T strategy and direction.

Answer: A

Explanation:

One of the objectives of CSF Step 6 is to translate improvement opportunities into justifiable, contributing projects, which means to develop an action plan that addresses the gaps between the current and target profiles, and that aligns with the organization's mission drivers, risk appetite, and resource constraints12.

Reference
Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide, page 8.
NIST CSF: The seven-step cybersecurity framework process

Question: 43

Which of the following is CRITICAL for the success of CSF Step 6: Determine, Analyze and Prioritize Gaps?

A. Identification of threats and vulnerabilities related to key assets
B. Experience in behavioral and change management
C. Clear understanding of the likelihood and impact of cybersecurity events

Answer: C

Explanation:

A clear understanding of the likelihood and impact of cybersecurity events is critical for the success of CSF Step 6, as it helps to prioritize the gaps and actions based on the risk assessment and the costbenefit analysis of

the proposed solutions12.

Reference

7 Steps to Implement & Improve Cybersecurity with NIST

NIST CSF: The seven-step cybersecurity framework process

Question: 44

Which of the following is MOST likely to cause an organization's NIST Cybersecurity Framework (CSF) implementation to fail?

A. Organizational training on the CSF is not provided.
B. Potential benefits of proposed improvements are not considered.
C. The implementation timeline is too long.

Answer: B

Explanation:

One of the most likely causes of an organization's NIST CSF implementation failure is that the potential benefits of proposed improvements are not considered, which means that the organization

does not conduct a cost-benefit analysis of the solutions to address the gaps between the current and target profiles. This can result in a lack of justification, prioritization, and alignment of the implementation plan with the organization's mission drivers, risk appetite, and resource constraints12.

Reference

7 Steps to Implement & Improve Cybersecurity with NIST

3 Security Issues Overlooked By the NIST Framework

Question: 45

Which function of the CSF is addressed by incorporating governance, risk, and compliance (GRC) elements into the implementation plan?

A. Protect
B. Detect
C. Identify

Answer: C

Explanation:

The function of the CSF that is addressed by incorporating governance, risk, and compliance (GRC) elements into the implementation plan is Identify, which assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities. GRC elements help to define the governance program, the legal and regulatory requirements, the risk management strategy, and the supply chain risk management strategy of the organization12. Reference

The Five Functions | NIST

NIST Cybersecurity Framework 2.0: Understanding the "Govern" Function

Question: 46

Which of the following is the MOST beneficial result of an effective CSF implementation plan?

A. Cybersecurity risk management practices are formalized and institutionalized.
B. Key stakeholders understand the quick wins of the cybersecurity program.
C. Key stakeholders understand the cybersecurity requirements of the chosen vendors.

Answer: A

Explanation:

The most beneficial result of an effective CSF implementation plan is that cybersecurity risk management practices are formalized and institutionalized, which means that the organization has established and maintained a consistent and comprehensive approach to managing cybersecurity risks across its systems, processes, and people. This result can help the organization to reduce the likelihood and impact of cybersecurity events, improve its resilience and compliance, and enhance its reputation and trust12.

Reference
Public Draft: The NIST Cybersecurity Framework 2, page 1.
Cybersecurity Framework | NIST

Question: 47

Which of the following is the PRIMARY reason for establishing open communication between all participants and stakeholders as part of the implementation phase?

A. To describe the high-level roadmap for achieving the vision
B. To ensure issues can be identified and resolved
C. To establish the sharing of information with external partners

Answer: B

Explanation:

The primary reason for establishing open communication between all participants and stakeholders as part of the implementation phase is to ensure issues can be identified and resolved, as this can facilitate the collaboration, coordination, and feedback among the involved parties, and help to overcome the challenges and risks that may arise during the implementation12.

Reference
Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA
Questions and Answers | NIST

Question: 48

During CSF life cycle action plan review, which of the following tasks is associated with realizing benefits?

A. Developing business cases indicating success factors

B. Monitoring performance against objectives
C. Documenting risk issues and remediation plans

Answer: B

Explanation:

According to the ISACA guide, monitoring performance against objectives is one of the tasks associated with realizing benefits, as it helps to measure the outcomes and value of the CSF implementation, and to identify and address any issues or gaps that may arise1. This task also involves reporting and communicating the results and feedback to the relevant stakeholders and ensuring continuous improvement2.

Reference

Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA

Manage Enterprise Cyberrisk by Applying the NIST CSF With COBIT ... - ISACA

Question: 49

The PRIMARY function of COBIT Implementation Phase 7: How Do We Keep the Momentum Going is to provide an opportunity for which of the following?

A. Closing the loop for communication workflow
B. Documenting improvements in a prioritized action plan
C. Ensuring frequent stakeholder communication

Answer: A

Explanation:

The primary function of COBIT Implementation Phase 7 is to provide an opportunity for closing the loop for communication workflow, which means to ensure that the results and feedback of the implementation are reported and communicated to the relevant stakeholders, and that the lessons learned and best practices are captured and shared for future reference12.

Reference

7 Phases in COBIT Implementation | COBIT Certification - Simplilearn

COBIT 2019 Design and Implementation COBIT Implementation, page 31.

Question: 50

Combining CSF principles with COBIT 2019 practices helps to ensure value, manage risk, and support mission drivers through support and direction of:

A. the chief information officer and IT management.
B. the board of directors and executive management.
C. the chief information security manager and the data protection officer.

Answer: B

Explanation:

Combining CSF principles with COBIT 2019 practices helps to ensure value, manage risk, and support mission drivers through support and direction of the board of directors and executive management, as they are responsible for setting the vision, strategy, and objectives of the organization, and for overseeing the governance and management of IT-related operations12.

Reference

Connecting COBIT 2019 to the NIST Cybersecurity Framework - ISACA

COBIT 2019 (With Principles, Components, Users and Benefits)