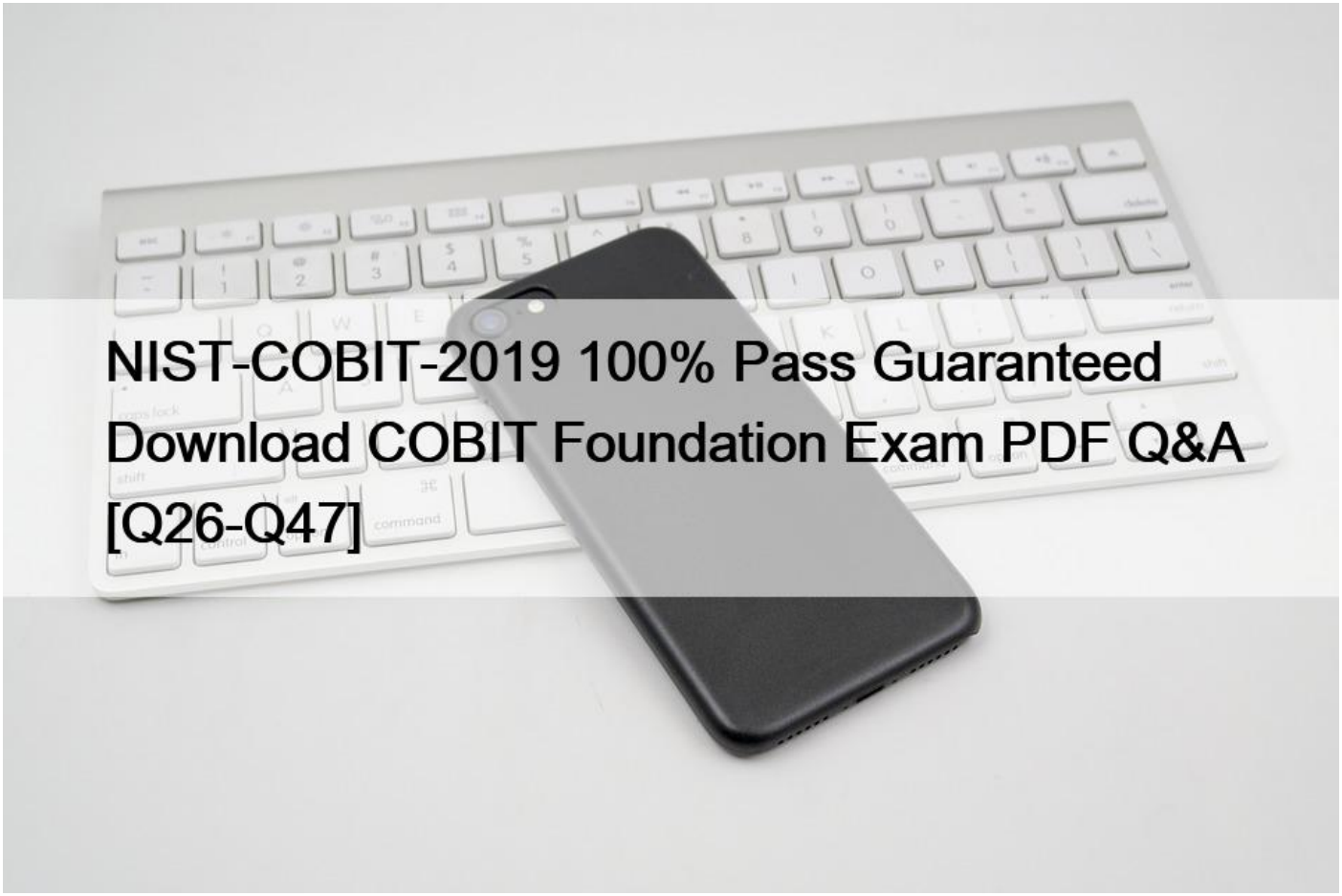
NIST-COBIT-2019 100% Pass Guaranteed Download COBIT Foundation Exam PDF Q&A [Q26-Q47



NIST-COBIT-2019 100% Pass Guaranteed Download COBIT Foundation Exam PDF Q&A NIST-COBIT-2019 Practice Test Dumps with 100% Passing Guarantee Q26. Which of the following is an objective of Implementation Phase 3 – Where Do We Want to Be?

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

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 .

References: 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

Q27. 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?
* Largely Achieved
* Partially Achieved
* Fully Achieved

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.

References:

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

Q28. The activity of determining an appropriate target capability level for each process occurs within which implementation phase?
* Phase 4 – What Needs to Be Done?
* Phase 3 – Where Do We Want to Be?
* Phase 2 – Where Are We Now?

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.

ReferencesDefining Target Capability Levels in COBIT 2019: A Proposal for RefinementCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

Q29. Analysis is one of the categories within which of the following Core Functions?
* Detect
* Respond
* Recover

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.

References: 1: The Five Functions | NIST 2: Cybersecurity Framework Components | NIST

Q30. Which of the following is CRITICAL for the success of CSF Step 6: Determine, Analyze and Prioritize Gaps?
* Identification of threats and vulnerabilities related to key assets
* Experience in behavioral and change management
* Clear understanding of the likelihood and impact of cybersecurity events

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 cost-benefit analysis of the proposed solutions12.

References7 Steps to Implement & Improve Cybersecurity with NISTNIST CSF: The seven-step cybersecurity framework process

Q31. Which information should be collected for a Current Profile?
* Implementation Status

* Recommended Actions
* Resource Required

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 References Not Applicable34.

References: 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.

Q32. Which of the following is a framework principle established by NIST as an initial framework consideration?

* Avoiding business risks
* Impact on global operations
* Ensuring regulatory compliance

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.

References: 1: Cybersecurity Framework | NIST 2: Framework Documents | NIST

Q33. Which of the following is an objective of COBIT Implementation Phase 3-Where Do We Want to Be?

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

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.

References: 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

Q34. Which of the following is an important consideration when defining the roadmap in COBIT Implementation Phase 3 – Where Do We Want to Be?

* Agreed metrics for measuring outcomes
* Reporting procedures and requirements
* Change-enablement implications

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.

References7 Phases in COBIT Implementation | COBIT Certification – SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

Q35. What does a CSF Informative Reference within the CSF Core provide?

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

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.

References: 1: Informative References: What are they, and how are they used? | NIST 2: Everything to Know About NIST CSF Informative References | Axio 3: NIST Cybersecurity Framework v1.1 – CSF Tools – Identity Digital

Q36. Which COBIT implementation phase directs the development of an action plan based on the outcomes described in the Target Profile?
* Phase 3 -Where Do We Want to Be?
* Phase 5 -How Do We Get There?
* Phase 4 -What Needs to Be Done?

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.

References7 Phases in COBIT Implementation | COBIT Certification – SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

Q37. Within the CSF Core structure, which type of capability can be implemented to help practitioners recognize potential or realized risk to enterprise assets?
* Protection capability
* Response capability
* Detection capability

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.

References: 1: The Five Functions | NIST 2: Cybersecurity Framework | NIST

Q38. Which of the following is a PRIMARY input into Steps 2 and 3: Orient and Create a Current Profile?
* Evaluating business cases
* Updating business cases
* Defining business cases

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.

References: 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

Q39. Which of the following COBIT tasks and activities corresponds to CSF Step 1: Prioritize and Scope?
* Understand the enterprise’s capacity and capability for change.
* Use change agents to communicate informally and formally.
* Determine ability to implement the change.

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.

References: 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

Q40. Which of the following is associated with the “Detect” core function of the NIST Cybersecurity Framework?
* Information Protection Processes and Procedures
* Anomalies and Events
* Risk Assessment

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.

References: 1: The Five Functions | NIST 2: Detect | NIST

Q41. The seven high-level CSF steps generally align to which of the following in COBIT 2019?
* High-level phases
* High-level functions
* High-level categories

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.

References: 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.

Q42. Identifying external compliance requirements is MOST likely to occur during which of the following COBIT implementation phases?
* Phase 4 – What Needs to Be Done?
* Phase 2 – Where Are We Now?
* Phase 3 – Where Do We Want to Be?

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.

References: 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

Q43. Which of the following should an organization review to gain a better understanding of the likelihood and impact of cybersecurity events?
* Relevant internal or external capability benchmarks

* Cybersecurity frameworks, standards, and guidelines
* Cyber threat information from internal and external sources

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.

ReferencesIdentifying and Estimating Cybersecurity Risk for Enterprise Risk Management, page 19.COBIT VS NIST : A Comprehensive Analysis – ITSM Docs

Q44. Which of the following is MOST important for successful execution of CSF implementation Step 6 – Determine, Analyze, and Prioritize Gaps?

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

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.

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

Q45. Documenting opportunities for improvement occurs within which implementation phase?

* Phase 4 – What Needs to Be Done?
* Phase 2 – Where Are We Now?
* Phase 3 – Where Do We Want to Be?

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.

References7 Phases in COBIT Implementation | COBIT Certification – SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.