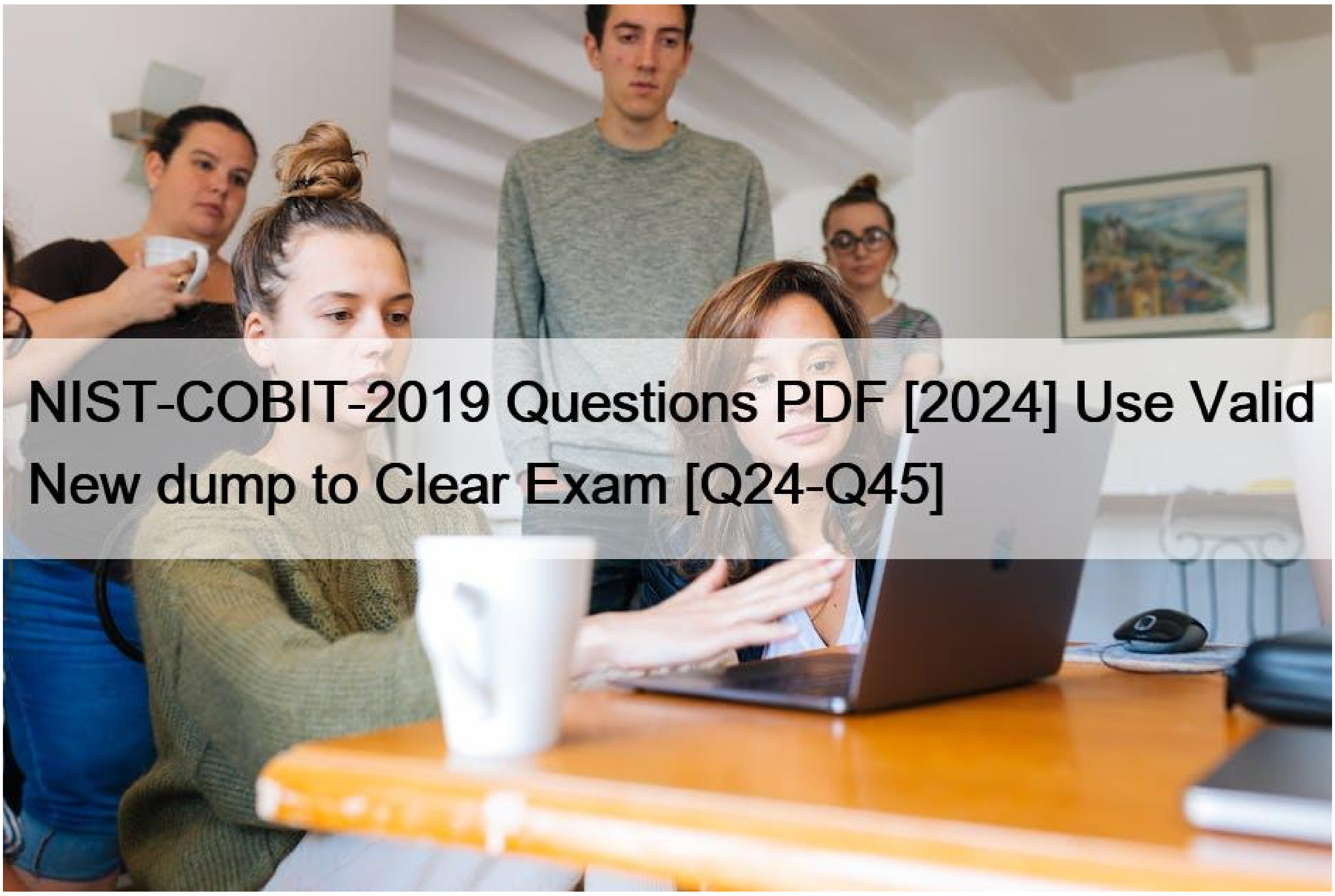
# NIST-COBIT-2019 Questions PDF [2024 Use Valid New dump to Clear Exam [Q24-Q45



**NIST-COBIT-2019 Questions PDF [2024 Use Valid New dump to Clear Exam Passing ISACA NIST-COBIT-2019 Exam Using 2024 Practice Tests QUESTION 24**

When aligning to the NIST Cybersecurity Framework, what should occur after tier levels and framework core outcomes are determined?
* Report discovered issues to senior management.
* Assign mitigating control development.
* Compare current and target profiles.
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&#8217;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.

ReferencesCybersecurity Framework Components | NISTWhat is the NIST Cybersecurity Framework? | IBM

**QUESTION 25**

Which of the following is one of the objectives of CSF Step 6: Determine, Analyze and Prioritize Gaps?
* Translate improvement opportunities into justifiable, contributing projects.
* Direct stakeholder engagement, communication, and reporting.
* Communicate the I&T strategy and direction.
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&#8217;s mission drivers, risk appetite, and resource constraints12.

ReferencesGetting Started with the NIST Cybersecurity Framework: A Quick Start Guide, page 8.NIST CSF:

The seven-step cybersecurity framework process

**QUESTION 26**

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

References7 Phases in COBIT Implementation | COBIT Certification &#8211; SimplilearnImplementing the NIST Cybersecurity Framework Using COBIT 2019, page 17.What is a Quick Win? &#8211; Definition from Techopedia

**QUESTION 27**

Which role will benefit MOST from a better understanding of the current cybersecurity posture by applying the CSF?
* Executives
* Acquisition specialists
* Legal experts
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.

References: 1: Implementing the NIST Cybersecurity Framework Using COBIT 2019 | ISACA 2:

Cybersecurity Framework | NIST 3: Framework Documents | NIST

**QUESTION 28**

What is the MOST important reason to compare framework profiles?
* To improve security posture
* To conduct a risk assessment
* To identify gaps
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.

References: 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 &#8211; ISACA

**QUESTION 29**

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 &#8211; 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 &#8211; SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

**QUESTION 30**

Documenting opportunities for improvement occurs within which implementation phase?
* Phase 4 &#8211; What Needs to Be Done?
* Phase 2 &#8211; Where Are We Now?
* Phase 3 &#8211; Where Do We Want to Be?
The objective of COBIT Implementation Phase 2 is to define the scope of the implementation using COBIT&#8217;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 &#8211; SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

**QUESTION 31**

Which of the following represents a best practice for completing CSF Step 3: Create a Current Profile?
* Procuring solutions that are cost-effective and fit the organization&#8217;s technical architecture
* Assessing current availability, performance, and capacity to create a baseline
* Engaging in a dialogue and obtaining input to determine appropriate goals, tiers, and Activities
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.

References: 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 32**

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 &#8211; ITSM Docs

**QUESTION 33**

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 &#8211; Testprep Training Tutorials

2: COBIT 2019 and COBIT 5 Comparison &#8211; ISACA

3: COBIT 2019 Performance Management: Principles and Processes

4: Effective Capability and Maturity Assessment Using COBIT 2019 &#8211; ISACA

**QUESTION 34**

Which of the following is MOST likely to cause an organization&#8217;s NIST Cybersecurity Framework (CSF) implementation to fail?
* Organizational training on the CSF is not provided.

* Potential benefits of proposed improvements are not considered.
* The implementation timeline is too long.
One of the most likely causes of an organization&#8217;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&#8217;s mission drivers, risk appetite, and resource constraints12.

References7 Steps to Implement & Improve Cybersecurity with NIST3 Security Issues Overlooked By the NIST Framework

**QUESTION 35**

Which of the following COBIT tasks and activities corresponds to CSF Step 1: Prioritize and Scope?
* Understand the enterprise&#8217;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&#8217;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 &#8220;Where are we now?&#8221;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 &#8211; ISACA 3: Connecting COBIT 2019 to the NIST Cybersecurity Framework &#8211; ISACA 4: Cybersecurity Framework Components | NIST

**QUESTION 36**

Combining CSF principles with COBIT 2019 practices helps to ensure value, manage risk, and support mission drivers through support and direction of:
* the chief information officer and IT management.
* the board of directors and executive management.
* the chief information security manager and the data protection officer.
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.

ReferencesConnecting COBIT 2019 to the NIST Cybersecurity Framework &#8211; ISACACOBIT 2019 (With Principles, Components, Users and Benefits)

**QUESTION 37**

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

**QUESTION 38**

The activity of determining an appropriate target capability level for each process occurs within which implementation phase?
* Phase 4 &#8211; What Needs to Be Done?
* Phase 3 &#8211; Where Do We Want to Be?
* Phase 2 &#8211; 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&#8217;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.

**QUESTION 39**

What does a CSF Informative Reference within the CSF Core provide?
* A high-level strategic view of the life cycle of an organization&#8217;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 &#8220;Maintain an inventory of IT assets&#8221;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 &#8211; CSF Tools &#8211; Identity Digital

**QUESTION 40**

Which of the following COBIT and NIST implementation steps may be reversed depending on the culture of the organization?
* Step 4: Conduct a Risk Assessment and Step 6: Determine, Analyze, and Prioritize Gaps
* Step 3: Create a Current Profile and Step 5: Create a Target Profile
* Step 1: Prioritize and Scope and Step 2: Orient
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.

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

**QUESTION 41**

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

**QUESTION 42**

Which of the following is an important consideration when defining the roadmap in COBIT Implementation Phase 3 &#8211; 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 &#8211; SimplilearnCOBIT 2019 Design and Implementation COBIT Implementation, page 31.

**QUESTION 43**

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.

**NIST-COBIT-2019 Study Guide Brilliant NIST-COBIT-2019 Exam Dumps PDF:**
https://www.validexam.com/NIST-COBIT-2019-latest-dumps.html]