Number: NIST-COBIT-2019
Passing Score: 800
Time Limit: 120
File Version: 3.0

Exam Code: NIST-COBIT-2019

Exam Name: ISACA Implementing the NIST Cybersecurity Framework using COBIT 2019

Exam A

QUESTION 1
Analysis is one of the categories within which of the following Core Functions?

A. Detect
B. Respond
C. Recover

Correct Answer: A
Section:
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.

QUESTION 2
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

Correct Answer: B
Section:
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 3
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.

Correct Answer: B
Section:
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.

QUESTION 4
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

Correct Answer: B
Section:
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 5
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

Correct Answer: C
Section:
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.

QUESTION 6
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

Correct Answer: B
Section:
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.

QUESTION 7
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

Correct Answer: C
Section:
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 8
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?

Correct Answer: B
Section:
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 9
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.

Correct Answer: A
Section:
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 10
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

Correct Answer: C
Section:
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 11
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

Correct Answer: A
Section:
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 12
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.

Correct Answer: B
Section:
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.

QUESTION 13
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.

Correct Answer: A
Section:
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.

QUESTION 14
Which of the following functions provides foundational activities for the effective use of the Cybersecurity Framework?

A. Protect
B. Identify
C. Detect

Correct Answer: B
Section:
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.

QUESTION 15
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

Correct Answer: C
Section:
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.

QUESTION 16
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

Correct Answer: A
Section:
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.

QUESTION 17
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

Correct Answer: C
Section:
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.

QUESTION 18
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.

Correct Answer: C
Section:
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.

QUESTION 19
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

Correct Answer: A
Section:
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.

QUESTION 20
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

Correct Answer: C
Section:
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.

QUESTION 21
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

Correct Answer: A
Section:
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 22
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.

Correct Answer: A
Section:
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.

QUESTION 23
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

Correct Answer: C
Section:
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.

QUESTION 24
Which information should be collected for a Current Profile?

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

Correct Answer: A
Section:
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 25
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

Correct Answer: C
Section:
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.

QUESTION 26
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?

Correct Answer: B
Section:
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.

QUESTION 27
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

Correct Answer: C
Section:
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.

QUESTION 28
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

Correct Answer: A
Section:
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.