

Exam Prep: Explore NIST Cybersecurity Framework and COBIT 2019

Understanding Cybersecurity Governance

In today's digital age, **cybersecurity** is more important than ever. Cybersecurity governance ensures that your organization can effectively protect its information and systems from potential threats. By combining the *NIST Cybersecurity Framework* with *COBIT 2019*, you can create a solid foundation for your cybersecurity strategy.

Exploring the NIST Cybersecurity Framework

The *NIST Cybersecurity Framework* is an essential guideline that helps organizations manage and reduce cybersecurity risk. It consists of five key functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. Understanding these functions is vital for any exam related to cybersecurity.

Why Use COBIT 2019?

COBIT 2019 is a framework that assists organizations in achieving their objectives, particularly concerning IT governance and management. Integrating *COBIT 2019* with the *NIST Cybersecurity Framework* allows you to enhance your cybersecurity approach while aligning IT with overall business goals. More information can be found on [this resource](#).

Implementing a Risk Management Framework

Risk management is crucial in cybersecurity. When studying for your exam, focus on how to develop an effective risk management framework. This should include **risk assessment**, **risk response**, and **continuous risk monitoring**.

Aligning with Information Security Standards

Using *information security standards* is key for any effective cybersecurity strategy. Familiarize yourself with common standards such as **ISO/IEC 27001**, which can complement your knowledge of *NIST* and *COBIT*. Knowing these standards can be beneficial not only for your exam but also for a career in cybersecurity.

Creating a Cybersecurity Strategy

To apply everything you've learned, you need to develop a **cybersecurity strategy**. Your strategy should encompass all aspects of the NIST framework and include governance elements from COBIT 2019. This comprehensive approach will ensure effective cybersecurity management.

Preparing for Your Exam

When preparing for your exam, consider the following tips:

- Review the *NIST Cybersecurity Framework* thoroughly.
- Understand the key components of *COBIT 2019*.
- Practice real-life scenarios of **cybersecurity governance**.
- Stay updated with the latest **information security standards**.
- Join study groups or forums to discuss relevant topics.
- Utilize online resources like [this link](#) for more insights.

Real Exam Questions 2025

Below given questions are for demo purposes only. **The full version** is up-to-date and contains actual questions and answers.

Why Choose CertKillers?

Actual Exam Questions: We provide real exam questions updated regularly.

Exam Dumps: Downloadable PDFs with comprehensive questions and answers.

Weekly Live updates: Study Material questions and answers – Live updates.

Practice Tests: Practice tests and VCE PDF to assess your readiness.

Multi-Lingual Support: Full Version products available for download in all popular languages.

Success Guarantee: Pass your exam on the first attempt or get a refund.

Up-To-Date Test Questions: Up-to-Date Test Prep Questions that cover 2025 syllabus.

Instant Download: Instant download after successful payment.

Visit CertKillers

[IBM-Truven-Micromedex-Technical-Sales-Mastery-v1.pdf](#)

[Implementation-Engineer-PowerEdge.pdf?target=b4d81f00-b4c3-410e-b91c-ba2a1b5c8367](#)

[ISACA-Implementing-the-NIST-Cybersecurity-Framework-using-COBIT-2019.pdf](#)

[Managing-Projects-with-Microsoft-Project-2013.pdf?target=cab2efab-e17e-468a-ad48-eca72767f1b6](#)

[Nokia-Triple-Play-Services.pdf?target=871b1d09-7c65-4b48-b1fb-6ce5a30939e3](#)

[Primavera-P6-Enterprise-Project-Portfolio-Manageme.pdf?target=31de8a0d-4998-40c4-9558-8ab0dde2200f](#)

[tpS6VcqBM47s4AjRISTQB-Certified-Tester-Foundation-Level-4.0.pdf](#)

[F2-Advanced-Financial-Reporting.pdf](#)

[x4cRKlQm47xKSafyState-Trooper-Certification-Exam.pdf](#)

[IBM-Tivoli-Application-Dependency-Discovery-Manage.pdf?target=44667cda-b018-43ed-82ac-cdb1131c91a5](#)



Isaca

NIST-COBIT-2019 Exam

**ISACA Implementing the NIST Cybersecurity Framework using
COBIT 2019**

Thank you for Downloading NIST-COBIT-2019 exam PDF Demo

You can Buy Latest NIST-COBIT-2019 Full Version Download

<https://www.certkillers.net/Exam/NIST-COBIT-2019>

<https://www.certkillers.net>

Version: 4.0

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 environment](#)⁴.

[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 capabilities](#)¹². [This understanding enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs](#)¹². [The Identify function includes outcome categories such as Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management](#)¹². [Reference: 1: The Five Functions | NIST 2: Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide](#)

Thank You for trying NIST-COBIT-2019 PDF Demo

To Buy New NIST-COBIT-2019 Full Version Download visit link
below

<https://www.certkillers.net/Exam/NIST-COBIT-2019>

Start Your NIST-COBIT-2019 Preparation

[Limited Time Offer] Use Coupon “CKNET” for Further discount on
your purchase. Test your NIST-COBIT-2019 preparation with actual
exam questions.

<https://www.certkillers.net>