Summary

The NIST Cybersecurity Framework (CSF) 2.0, released in February 2024, is a flexible, voluntary framework designed to help organizations of all sizes and sectors manage cybersecurity risks. It comprises the CSF Core (a taxonomy of high-level cybersecurity outcomes organized into Functions, Categories, and Subcategories), Organizational Profiles (for describing current or target cybersecurity posture), and Tiers (to characterize the rigor of risk governance). The CSF defines desirable outcomes but does not prescribe specific implementation methods, instead leveraging a suite of online resources for detailed guidance. It enables organizations to understand, assess, prioritize, and communicate cybersecurity risks globally.

Key Points

- ★ NIST CSF 2.0 is a flexible framework for managing cybersecurity risks, applicable to all organization types and sizes globally, regardless of maturity level.
- ★ The CSF includes three main components: the CSF Core (a taxonomy of outcomes organized into Functions, Categories, and Subcategories), CSF Organizational Profiles (to describe current/target cybersecurity posture), and CSF Tiers (to characterize risk governance rigor).
- ★ The CSF outlines desirable cybersecurity outcomes but does not prescribe specific methods or controls for achieving them; detailed guidance is provided through online resources.
- ★ Complementary online resources include Informative References, Implementation Examples, Quick-Start Guides, Community Profiles, and Organizational Profile Templates.
- ★ Organizations use the CSF to understand and assess, prioritize, and communicate cybersecurity risks.
- ★ The CSF Core is structured around six high-level Functions: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER.
- ★ The GOVERN Function establishes the organization's cybersecurity risk management strategy and integrates cybersecurity into broader enterprise risk management (ERM).
- ★ The IDENTIFY Function focuses on understanding current cybersecurity risks, including an organization's assets, suppliers, and related risks.

Multiple Choice Questions

1. What are the hierarchical components that form the CSF Core's taxonomy of cybersecurity outcomes?

a) Policies, Procedures, and Standards

b) Inputs, Processes, and Outputs

c) Functions, Categories, and Subcategories

d) Regulations, Guidelines, and Mandates

Answer: c

Explanation: The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome.

2. Which statement accurately describes the NIST CSF 2.0's approach to achieving cybersecurity outcomes?

a) It prescribes specific technologies and methods organizations must use.

b) It outlines desirable outcomes but does not prescribe how they should be achieved.

c) It mandates a fixed sequence of actions for all organizations regardless of their unique risks.

d) It solely focuses on regulatory compliance without offering flexibility for customization.

Answer: b

Explanation: The document states that the CSF describes what desirable outcomes an organization can aspire to achieve, but it does not prescribe outcomes nor how they may be achieved.

3. What is the primary purpose of CSF Tiers?

a) To provide a checklist of mandatory cybersecurity actions for all organizations.

b) To categorize organizations by their industry sector or size for benchmarking.

c) To characterize the rigor of an organization's cybersecurity risk governance and management practices.

d) To define specific financial investments required for cybersecurity improvements.

Answer: c

Explanation: CSF Tiers are applied to CSF Organizational Profiles to characterize the rigor of an organization’s cybersecurity risk governance and management practices.

4. Which of the following is NOT listed as a way an organization can use the CSF with supplementary resources?

a) Understand and Assess cybersecurity posture.

b) Prioritize actions for managing cybersecurity risks.

c) Mandate specific vendor solutions for cybersecurity implementation.

d) Communicate cybersecurity risks, capabilities, and needs.

Answer: c

Explanation: The document states organizations can use the CSF to Understand and Assess, Prioritize, and Communicate cybersecurity risks. It does not mention mandating specific vendor solutions.

5. The NIST CSF is designed to be used by which of the following?

a) Only large government agencies and critical infrastructure operators.

b) Primarily US-based organizations with high cybersecurity maturity.

c) Organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, globally.

d) Organizations that are legally mandated to adopt the framework.

Answer: c

Explanation: The CSF is designed to be used by organizations of all sizes and sectors, including industry, government, academia, and nonprofit organizations, regardless of maturity level, and has been leveraged successfully both inside and outside the United States.

6. Which of these is a type of online resource that complements the CSF and offers additional guidance?

a) Mandatory audit reports for compliance checks.

b) Competitive benchmarking tools for industry comparison.

c) Informative References that point to sources of guidance from existing global standards.

d) Financial cost calculators for cybersecurity investments.

Answer: c

Explanation: The text lists Informative References, Implementation Examples, Quick-Start Guides, and Community Profiles as types of online resources that complement the CSF.

7. What is the primary focus of the GOVERN (GV) Function in the CSF Core?

a) To detect cybersecurity incidents in real-time.

b) To establish the organization’s cybersecurity risk management strategy and integrate it into broader enterprise risk management (ERM).

c) To recover data and systems after a cybersecurity incident.

d) To implement protective technical controls for systems and data.

Answer: b

Explanation: The GOVERN Function provides outcomes to inform what an organization may do to achieve and prioritize the outcomes of the other five Functions, and is critical for incorporating cybersecurity into an organization’s broader enterprise risk management (ERM) strategy.

8. The IDENTIFY (ID) Function of the CSF Core primarily helps an organization to:

a) Develop new cybersecurity technologies and tools.

b) Understand its current cybersecurity risks, including its assets, suppliers, and related risks.

c) Respond to an active cyberattack and minimize damage.

d) Create incident response plans without assessing current assets.

Answer: b

Explanation: The IDENTIFY Function focuses on understanding the organization’s assets, suppliers, and related cybersecurity risks to prioritize its efforts consistent with its risk management strategy.

9. How many distinct Functions are there in the CSF Core?

a) Three

b) Four

c) Five

d) Six

Answer: d

Explanation: The CSF Core Functions are GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER, totaling six functions.

10. Regarding the CSF's flexibility, which statement is true?

a) It mandates a one-size-fits-all approach for all organizations to ensure consistency.

b) It is intended to be tailored for use by all organizations regardless of size, acknowledging unique risks and objectives.

c) It only applies to organizations with identical risk tolerances and mission objectives.

d) It eliminates the need for organizations to consider their unique mission objectives and requirements.

Answer: b

Explanation: The CSF is a flexible framework that is intended to be tailored for use by all organizations regardless of size, recognizing that organizations will continue to have unique risks and mission objectives.