◇ EASY (Q1–Q10)

Q1. The primary objective of the NIST Cybersecurity Framework is to:
A. Certify organizations
B. Eliminate cyber attacks
C. Manage and reduce cybersecurity risk
D. Replace all security standards

Q2. NIST is an organization based in which country?
A. United Kingdom
B. European Union
C. United States
D. Japan

Q3. The NIST Cybersecurity Framework is best described as:
A. A mandatory law
B. A risk-based framework
C. A technical configuration guide
D. A certification scheme

Q4. How many core functions are defined in the NIST CSF?
A. Three
B. Four
C. Five
D. Seven

Q5. Which of the following is NOT a NIST CSF core function?
A. Identify
B. Protect
C. Audit
D. Recover

Q6. The “Identify” function primarily focuses on:
A. Incident handling
B. Understanding organizational risk
C. System recovery
D. Security testing

Q7. NIST CSF is most suitable for:
A. Only government agencies
B. Only large enterprises
C. Organizations of all sizes
D. Only financial institutions

Q8. NIST CSF is considered voluntary because it:
A. Has no controls
B. Is not legally binding
C. Cannot be audited
D. Is outdated

Q9. Which NIST CSF function deals with incident containment?
A. Protect
B. Detect
C. Respond
D. Recover

Q10. NIST CSF primarily supports which security approach?
A. Tool-based
B. Checklist-based
C. Risk-based
D. Incident-only

◇ MEDIUM (Q11–Q25)

Q11. The NIST CSF core is organized into:
A. Policies and standards
B. Functions, categories, and subcategories
C. Controls and checklists
D. Laws and regulations

Q12. Which function of NIST CSF emphasizes early identification of cybersecurity events?
A. Identify
B. Protect
C. Detect
D. Recover

Q13. Implementation Tiers in NIST CSF describe:
A. Network layers
B. Maturity of risk management practices
C. Levels of certification
D. Compliance scores

Q14. Which NIST Implementation Tier reflects continuous improvement?
A. Tier 1 – Partial
B. Tier 2 – Risk-Informed
C. Tier 3 – Repeatable
D. Tier 4 – Adaptive

Q15. A NIST Profile is used to:
A. Replace audits
B. Align cybersecurity activities with business needs
C. Perform vulnerability scans
D. Certify compliance

Q16. Which profile represents an organization's desired cybersecurity state?
A. Baseline Profile
B. Current Profile
C. Target Profile
D. Compliance Profile

Q17. The "Protect" function mainly addresses:
A. Risk identification
B. Preventive safeguards
C. Incident reporting
D. System restoration

Q18. NIST CSF best supports governance by:
A. Enforcing penalties
B. Providing a common risk language
C. Eliminating threats
D. Automating security

Q19. Which stakeholder MOST benefits from NIST CSF reporting?
A. End users
B. Board and senior management
C. Attackers
D. Vendors only

Q20. NIST CSF categories are further divided into:
A. Controls
B. Requirements
C. Subcategories
D. Clauses

Q21. Which NIST CSF function focuses on resilience and continuity?
A. Protect
B. Detect
C. Respond
D. Recover

Q22. NIST CSF is particularly useful for organizations because it is:
A. Prescriptive
B. Technology-neutral
C. Vendor-specific
D. Certification-oriented

Q23. Which risk management concept is central to NIST CSF?
A. Zero trust only
B. Residual risk
C. Risk appetite and tolerance
D. Penetration testing

Q24. Which document series published by NIST provides detailed guidance?
A. ISO 27000 series
B. COBIT publications
C. SP 800 series
D. PCI DSS manuals

Q25. The main limitation of NIST CSF is that it:
A. Is too technical
B. Is not certifiable
C. Ignores governance
D. Is outdated

△ HARD (Q26–Q40)

Q26. Which scenario BEST demonstrates use of NIST CSF Profiles?
A. Installing firewalls
B. Comparing current security posture with desired state
C. Conducting penetration testing
D. Auditing financial controls

Q27. An organization operating at Tier 2 (Risk-Informed) MOST likely has:
A. Ad-hoc security practices
B. Fully optimized controls
C. Awareness of risk but inconsistent implementation
D. Continuous automated monitoring

Q28. Which feature differentiates NIST CSF from ISO/IEC 27001 MOST clearly?
A. Risk orientation
B. Certification capability
C. Governance focus
D. Control mapping

Q29. The NIST CSF “Detect” function contributes MOST to:
A. Risk elimination
B. Early threat visibility
C. Policy development
D. Business alignment

Q30. NIST CSF supports compliance by:
A. Replacing legal requirements
B. Mapping controls to regulations
C. Issuing compliance certificates
D. Enforcing penalties

Q31. A highly regulated organization prefers NIST CSF because it:
A. Is rigid
B. Is adaptable to regulations
C. Eliminates audits
D. Guarantees compliance

Q32. Which governance weakness reduces effectiveness of NIST adoption?
A. Defined risk appetite
B. Board involvement
C. Lack of leadership commitment
D. Regular reviews

Q33. NIST CSF encourages which security philosophy?
A. Reactive security
B. Preventive security only
C. Lifecycle-based risk management
D. Tool-centric defense

Q34. Which function MOST supports executive-level cyber reporting?
A. Detect
B. Protect
C. Identify
D. Respond

Q35. An organization using NIST CSF without risk assessment will MOST likely:
A. Achieve maturity
B. Misalign controls with threats
C. Optimize investments
D. Improve assurance

Q36. Which statement BEST describes NIST CSF’s relationship with audits?
A. Replaces audits
B. Eliminates compliance needs
C. Complements audits with risk context
D. Conflicts with audits

Q37. Which factor MOST influences the selection of NIST Implementation Tier?
A. Number of employees
B. Organization’s risk tolerance
C. IT infrastructure size
D. Budget alone

Q38. The NIST CSF is MOST valuable in which situation?
A. Static environments
B. Rapidly evolving threat environments
C. Small offline organizations
D. Non-digital businesses

Q39. Which NIST CSF function MOST directly links cybersecurity to business objectives?
A. Detect
B. Protect
C. Identify
D. Recover

Q40. The PRIMARY value of the NIST CSF is that it:
A. Guarantees security
B. Provides structured risk management guidance
C. Automates compliance
D. Replaces all standards