## ◇ EASY (Q1–Q10)

**Q1.** PCI DSS primarily aims to protect:
A. Intellectual property
B. Cardholder data
C. Network bandwidth
D. Software source code

**Q2.** PCI DSS is governed by which organization?
A. ISO
B. NIST
C. PCI Security Standards Council
D. AICPA

**Q3.** PCI DSS applies to organizations that:
A. Are publicly listed
B. Process, store, or transmit card data
C. Provide IT services only
D. Operate banks only

**Q4.** Which data element is considered cardholder data?
A. Customer address only
B. Primary Account Number (PAN)
C. Merchant ID
D. Transaction timestamp

**Q5.** PCI DSS is best described as a:
A. Law
B. Industry-mandated security standard
C. Voluntary guideline
D. Certification framework

**Q6.** PCI DSS compliance is enforced primarily through:
A. Courts
B. Government regulators
C. Contractual obligations with card brands
D. ISO certification

**Q7.** Which of the following is NOT a PCI DSS objective?
A. Protect cardholder data
B. Reduce payment fraud
C. Ensure high system performance
D. Secure payment environments

**Q8.** PCI DSS requirements are organized around how many major objectives?
A. 4
B. 5
C. 6
D. 12

**Q9.** PCI DSS applies to which transaction type?
A. Only online payments
B. Only physical card transactions
C. All card-based transactions
D. Only international transactions

**Q10.** Which entity ultimately bears responsibility for PCI DSS compliance?
A. Payment processor only
B. Card brands
C. Merchant handling card data
D. External auditor

---

## ◇ MEDIUM (Q11–Q25)

**Q11.** PCI DSS merchant compliance levels are primarily based on:
A. Number of employees
B. Annual transaction volume
C. Organization revenue
D. IT infrastructure size

**Q12.** A Level 1 merchant typically processes:
A. Less than 20,000 transactions per year
B. 20,000 to 1 million transactions
C. 1 to 6 million transactions
D. Over 6 million transactions

**Q13.** Which PCI DSS requirement focuses on access control?
A. Requirement 1
B. Requirement 4
C. Requirement 7
D. Requirement 11

**Q14.** Which PCI DSS requirement addresses vulnerability management?
A. Requirement 1
B. Requirement 3
C. Requirement 5
D. Requirement 12

**Q15.** Self-Assessment Questionnaires (SAQs) are typically used by:
A. Level 1 merchants only
B. All service providers
C. Lower-level merchants
D. Card brands

**Q16.** Which PCI DSS report is completed after an external audit?
A. Attestation of Compliance (AOC)
B. Risk register
C. Gap analysis report
D. SOC report

**Q17.** Which PCI DSS objective focuses on monitoring and testing networks?
A. Objective 2
B. Objective 4
C. Objective 5
D. Objective 6

**Q18.** Which data type must NEVER be stored after authorization?
A. PAN
B. Cardholder name
C. CVV/CVC
D. Expiry date

**Q19.** Which requirement MOST directly supports incident detection?
A. Requirement 6
B. Requirement 8
C. Requirement 10
D. Requirement 12

**Q20.** PCI DSS requires organizations to maintain which type of policy?
A. Data privacy policy only
B. Information security policy
C. HR policy
D. Backup policy only

**Q21.** PCI DSS applies to service providers because they:
A. Own card brands
B. Handle cardholder data on behalf of merchants
C. Provide auditing services
D. Are government entities

**Q22.** Which PCI DSS validation method is MOST rigorous?
A. SAQ
B. ROC (Report on Compliance)
C. Internal checklist
D. Vendor questionnaire

**Q23.** Which PCI DSS principle MOST aligns with defense-in-depth?
A. Single control enforcement
B. Layered security controls
C. Encryption only
D. Physical security only

**Q24.** PCI DSS compliance reviews are typically conducted:
A. Once in a lifetime
B. Every five years
C. Annually
D. Only after breaches

**Q25.** Which role performs PCI DSS external assessments?
A. Internal auditor
B. Qualified Security Assessor (QSA)
C. System administrator
D. Developer

---

## △ HARD (Q26–Q40)

**Q26.** An organization outsourcing payment processing still remains responsible for PCI DSS because:
A. Responsibility is fully transferable
B. Card brands enforce shared accountability
C. Compliance responsibility cannot be outsourced
D. Vendors guarantee compliance

**Q27.** Which scenario BEST indicates PCI DSS scope creep?
A. Limiting card data environment
B. Poor network segmentation
C. Encrypting PAN
D. Annual audits

**Q28.** Which failure MOST increases PCI DSS non-compliance risk?
A. Strong vendor contracts
B. Inadequate asset inventory
C. Regular vulnerability scans
D. Incident response testing

**Q29.** PCI DSS Requirement 12 primarily addresses:
A. Encryption
B. Firewall configuration
C. Security policy and governance
D. Malware protection

**Q30.** Which challenge MOST affects PCI DSS compliance in cloud environments?
A. Fixed infrastructure
B. Shared responsibility ambiguity
C. Reduced threat exposure
D. Limited scalability

**Q31.** Which PCI DSS control objective MOST directly reduces fraud risk?
A. Monitoring access logs
B. Protecting stored cardholder data
C. Backup and recovery
D. Change management

**Q32.** Treating PCI DSS as a checklist MOST often results in:
A. Improved security posture
B. Superficial compliance
C. Optimized governance
D. Reduced audit scope

**Q33.** Which PCI DSS requirement MOST supports accountability?
A. Requirement 3
B. Requirement 7
C. Requirement 10
D. Requirement 12

**Q34.** A merchant failing to maintain compliance MOST likely faces:
A. Criminal prosecution
B. Contractual fines and penalties
C. Loss of certification only
D. No consequences

**Q35.** Which PCI DSS concept MOST supports risk-based security?
A. Annual audits
B. Scope reduction
C. Control prioritization
D. Transaction monitoring

**Q36.** Which PCI DSS requirement MOST supports forensic investigations?
A. Requirement 2
B. Requirement 5
C. Requirement 10
D. Requirement 11

**Q37.** PCI DSS complements ISO/IEC 27001 by providing:
A. Enterprise-wide governance
B. Payment-specific security controls
C. Certification framework
D. Risk management model

**Q38.** Which governance weakness MOST undermines PCI DSS effectiveness?
A. Executive oversight
B. Poor documentation
C. Lack of security culture
D. Regular reviews

**Q39.** Which PCI DSS compliance level has the HIGHEST validation requirements?
A. Level 4
B. Level 3
C. Level 2
D. Level 1

**Q40.** The PRIMARY objective of PCI DSS is to:
A. Replace banking regulations
B. Protect cardholder data and reduce fraud
C. Ensure high transaction speed
D. Eliminate all payment risks