Question Bank 2023-24

MCQ on Digital Payment Security Policy

Q.1 What is the primary objective of the Digital Payment Security Policy?

A. Maximizing customer service disruption
B. Aligning with the overall business strategy
C. Ignoring regulatory compliance
D. Neglecting risk management

ANS: B

Q.2 Which department is responsible for owning and implementing the Digital Payment Security Policy?

A. CO: Fraud Risk Division
B. CO: Digital Banking Division
C. CO: IT Strategy Committee
D. CO: Customer Service Division

ANS: B

Q.3 Bank shall conduct a periodic overhaul review _____of its IT and IT Security architecture and technology platform based on Board-approved policy.

A. at least once in a year
B. at least once in a 2 year
C. at least once in a 5 year
D. at least once in a 6 Month

ANS: A

Q.4 Bank shall implement secure standard communication protocol in the digital payment channels (especially over Internet).The level of encryption should be as recommended by

A. RBI
B. CERT-In
C. IDRBT
D. Cyber Security Protocol Cell

ANS: B

Q.5 CISO should ensure implementation of this policy and place note to ITSC on _____ basis on implementation of the policy.

A. Monthly
B. Bimonthly
C. Quaterly
D. Half yearly

ANS: C

Question Bank 2023-24

MCQ on Digital Payment Security Policy

Q.7 The New product/process shall be approved by New Product/process Approval Committee(NPPAC) and _____ . _____ clearance shall be obtained before rolling-out the product/process

A. FRMC ,MD AND CEO
B. ORMC, Board
C. ORMC,CISO
D. FRMC,CISO

ANS: C

Q.8 Bank shall implement_____ and DDoS mitigation techniques to secure the digital payment products and services offered over Internet.

A. Web Application Firewall (WAF) solution
B. TCP IP
C. CISO protocol
D. IDRBT techniques

ANS: A

Q.9 Which standard is NOT mentioned in the context of application security?

A. OWASP-MASVS
B. ISO 12812
C. PCI-DSS
D. NIST

ANS: C

Q.10 Bank should also implement appropriate measures to minimize exposure to a middleman attack which is more commonly known as _____

A. MITM Attack
B. MITB Attack
C. MITA Attack
D. All the above 3

ANS: D

Q.11 Bank shall conduct vulnerability assessment (VA) of its digital payment applications at least on a _____ basis and penetration testing (PT) on at least _____ basis

A. bi-annual , annual
B. annual , bi-annual
C. annual , annual
D. bi- annual , bi-annual

ANS: A

Question Bank 2023-24

MCQ on Digital Payment Security Policy

Q.13 Bank shall implement Technology operations practices _____

A. system security management
B. network management and security backup management
C. vulnerability assessment and penetration testing, patch management
D. All the above

ANS: D

Q.14 What committee is responsible for approving new digital payment products?

A. Information Security Steering Committee
B. Digital Banking Division
C. New Product/process Approval Committee
D. Risk Management Committee

ANS: C

Q.15 What is the responsibility of Bank regarding suspicious transactions?

A. Ignore them for customer privacy
B. Review quarterly without alerts
C. Periodically update fraud rules
D. Only monitor during business hours

ANS: C
