ricago™

GRC BULLETIN

SEPTEMBER - 2024, VOLUME: I

RBI

Master directions on cyber resilience and digital payment security controls for Nonbank payment system operators

Click Here to Read Full Bulletin

#Trusted Compliance Partner

RBI – MASTER DIRECTIONS ON CYBER RESILIENCE AND DIGITAL PAYMENT SECURITY CONTROLS FOR NONBANK PAYMENT SYSTEM OPERATORS

Applicability:

Applicable to all authorized non-bank Payment System Operators (PSOs) in India.

The "Master Directions on Cyber Resilience and Digital Payment Security Controls for non-bank Payment System Operators" issued by the Reserve Bank of India (RBI). These directions are intended to enhance the security and resilience of digital payment systems operated by non-bank Payment System Operators (PSOs) against various cyber threats and vulnerabilities.

Key Highlights:

- PSOs must have a Board-approved Information Security (IS) policy.
- The Board is responsible for overseeing cyber risks, though a sub-committee may handle day-to-day oversight.
- A senior executive, like a Chief Information Security Officer (CISO), must manage the implementation of IS policies.
- PSOs are required to prepare a Cyber Crisis Management Plan (CCMP) to handle cyber threats.
- Regular risk assessments and monitoring must be conducted, especially when launching new products or services.
- Comprehensive inventory management of all key roles, assets, and critical functions.
- Implementation of strict identity and access management protocols.
- Network security measures including multi-layered defenses, Security Operations Centres (SOC), and automated threat detection tools.
- Secure application development and rigorous security testing (e.g., vulnerability assessments, penetration testing).
- Vendor risk management, particularly for critical processes and data protection.
- PSOs must have an incident response mechanism in place, including post-incident analysis and reporting to the RBI and CERT-In.

#

CORPORATE LAWS

Authority

Reserve Bank of India

Circular Date

July 30, 2024

Circular Number

RBI/DPSS/2024-25/123
CO.DPSS.OVRST.No.S4
47/06-26-002/2024-25

Effective Date

July 30, 2024

CORPORATE LAWS

- A robust Business Continuity Plan (BCP) must be developed to ensure rapid recovery from cyber incidents.
- Specific provisions for cloud security, employee awareness and training, and securing Application Programming Interfaces (APIs).
- Payment transactions involving debits to accounts must be validated through multi-factor authentication.

SOURCE: Click Here for more details

Authority

Reserve Bank of India

Circular Date

July 30, 2024

Circular Number

RBI/DPSS/2024-25/123
CO.DPSS.OVRST.No.S4
47/06-26-002/2024-25

Effective Date

July 30, 2024

ricago™

Head Quarters:

Vasudha, 2nd Floor, No. 2, 38th Main Rd, Rose Garden, JP Nagar Phase 6, J. P. Nagar, Bengaluru, Karnataka 560078

Ph: 080 41673023

Email: info@ricago.com

Website: www.ricago.com

Subscribe to the Newsletter: Subscribe

#Trusted Compliance Partner