CyRAACS™
Your Trusted Security Partner

RBI MASTER DIRECTION ON DIGITAL PAYMENT SECURITY CONTROLS

1.INTRODUCTION

As the digital payment footprint increases and cybercrime incidents rise in India, Reserve Bank of India has decided to tighten the security measures by introducing RBI's Master Direction on Digital Payments Security Controls. This comes at a crucial time when there is a huge spike in instances of outages, online fraud, and data leaks.

Addressing this growing issue in the finance industry, RBI's Master Direction comes as a guideline for Regulated Entities such as the Scheduled Commercial Banks, Small Finance Banks, Payment Banks, and Credit Card issuing NBFCs to implement an effective governance structure and establish industry standards of security controls for digital payment products and services.

While the guidelines will be technology and platform agnostic, it will create an enhanced and enabling environment for customers to use digital payment products in more safe and secure manner.

2.APPLICABILITY

The Master Direction applies to the following Regulated Entities (REs):

- **Scheduled Commercial Banks (excluding Regional Rural Banks)**
- **Payments Banks**
- **Small Finance Banks**
- **Credit card issuing NBFCs**

3.TIMELINES

The Reserve Bank of India's Master Direction was released on February 18, 2021. The guidelines will come into effect from August 2021, 6 months from the date of issue

4.CONTROL REQUIREMENTS

The Master Direction has detailed control requirements defined for various security aspects. These are broadly categorized as

- **General Controls**
  1. Governance and Management of Security Risks
  2. Other Generic Security Controls
  3. Application Security Life Cycle (ASLC) Controls
  4. Authentication Framework
  5. Fraud Risk Management
  6. Reconciliation Mechanism
  7. Customer Protection, Awareness and Grievance Redressal Mechanism
- **Internet Banking Security Controls**
- **Mobile Payments Application Security Controls**
- **Card Payments Security Controls**

5.KEY ACTIVITIES FOR COMPLIANCE

Some of the key controls to be implemented are:

1. Digital payment products and services Policy
2. Risk Management program for digital payment products and services
3. Security Risk Assessments
4. Security controls for databases and applications storing customer data
5. Web Application Firewall (WAF)and DDoS Mitigation implemention
6. 'Secure by Design' approach for digital payment products development
7. Source Code Review
8. Vulnerability Assessment (VA) and Penetration Testing (PT)
9. Security Testing for APIs
10. Customer information redation/ masking
11. Adaptive Authentication and Maximum failed login attempts
12. Multi-Factor Authentication for payments
13. System alerts for fraud risks, fraud analysis
14. Real time/near-real time reconciliation framework
15. Updated contact details of service providers, intermediaries, and external agencies
16. Secure, safe, and responsible usage guidelines and training materials
17. Additional levels of authentication for internet banking website
18. Terminate Online Sessions after fixed period of inactivity
19. Mobile Application version verification before transactions
20. Device Policy Enforcement for app installation
21. Device binding of mobile application
22. Implementation of payment card standards
23. Security measures for ATM
24. Robust surveillance/ monitoring of card transactions

6.How can CyRAACS Help You

CyRAACS can help you achieve compliance to the requirements of the Master Direction through a phased approach.

As part of the engagement, CyRAACS will conduct a Gap Assessment against requirements of the Master Direction and provide recommendations to fix the gaps identified. Additionally, CyRAACS will help to develop appropriate security policies and processes to fix the gaps.

Once the recommendations from the Gap Assessment have been fixed, CyRAACS will conduct a Validation Assessment and provide a Report of Compliance.

7.Why CyRAACS

- Empaneled with Indian Computer Emergency Response Team (CERT-In) as Information Security Auditor
- Proven track record of delivering complex projects across varied domains such as BFSI, Born-in-the-Cloud, Logistics, IT/ITES, Manufacturing, Pharma etc
- Extensive experience in Information Security and Data Privacy Standards/Frameworks such as ISO 27001, RBI Cybersecurity Framework, NIST 800-53, CSA STAR, GDPR, CCPA etc
- Over 200 happy clients and 500+ successful engagement deliveries
- Cyber Security Solutions tailor-made to Client requirements
- Consultants with Leading Industry Certifications CISSP, OSCP, CISA, CEH, CISM etc

ASSESSMENT PROCESS

Information Gathering

Gap Assessment

Information Security Compliance Framework

Validation Assessment

+91 98862 10050 | www.cyraacs.com | ms@cyraacs.com