VISTA INFOSEC®

TRUSTED ADVISORS, ASSURED COMPLIANCE™

RBI's Master Direction on Digital Payment Security Controls

W: www.vistainfosec.com
E: info@vistainfosec.com

US Tel: +1-415-513-5261 | SG Tel: +65-3129-0397 |
IN Tel: +91 73045 57744

An ISO27001 Certified Company, CERT-IN Empanelled, PCI QSA | **USA. SINGAPORE. INDIA. UK. MIDDLE EAST. CANADA.**

Topics Covered

Introduction

Given the dynamic digital landscape and skyrocketing online payment transactions, the industry has witnessed huge spike in cybercrimes. Addressing the growing need for stringent digital payment security controls in the industry, RBI recently issued a comprehensive Master Direction for organizations to follow. The Master Direction works as a guideline for organizations to improve the security, and governance of payment gateways, wallets, and other digital payment transactions that they deal with on a day-to-day basis.

The guidelines will help organizations establish a robust digital payment system and implement effective standards of security controls for online payments. With this Master Direction, it is now expected that entities like banks and NBFC's emphasise on their quality of governance, risk management, and internal security controls for establishing a safer digital payment environment. The issued guidelines specify security protocols to be implemented in mobile applications, internet banking, and card payments by scheduled commercial banks, small financial and payment banks, and card issuing institutes.

The Master Direction is issued at crucial time when the financial industry is in the mid of its rapid digital transformation and evolving security landscape. The guidelines issued is a technological and application-based framework that improves the digital payment environment for customers to securely embrace the evolving digitization of the financial industry. While this initiative is seen as a positive move to towards strengthening the regulations and supervision, it is yet to be seen as to how the enforcement of the security framework takes it course.

Key Highlights of the Master Direction

It provides a comprehensive governance structure and minimum-security control standards for systems like internet banking, mobile banking, card payment, etc.

It is a Standard driven by secure and robust security governance controls of international standards and guidelines like OWASP, NIST, ISO, PCI to name a few.

It contains requirements for strong governance, implementation, and monitoring of security control standards by scheduled commercial banks, small financial and payment banks, and card issuing institutes.

The Master Directions will also have implications on the third-party payment applications such as Google Pay, PhonePe, etc.

RBI's Master Direction covers a diverse area, including important security controls concerning the Governance and Management of Security Risks, Generic Security Controls, Application Security Life Cycle (ASLC), Authentication Framework, Fraud Risk Management, Reconciliation Mechanism, Customer Protection, Awareness and Grievance Redressal Mechanism related to Internet Banking, Mobile Payments Application Security Controls, and Card Payments Security.

It will come into effect on August which is six months from the day they are placed on the official website of the Reserve Bank of India (RBI). The timeline would be with immediate effect from thereon.

Applicability of the Master Direction

It provides a comprehensive governance structure and minimum-security control standards for systems like internet banking, mobile banking, card payment, etc.

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

Typically speaking the issued guidelines will also affect the business models of several payment gateways. The directions will have implications on third-party payment applications such as Google Pay, PhonePe, etc.

Timeline

The guidelines is set to come into full effect from **August 2021 (6 months post-release of the guidelines)**

Objective of the Master Direction

The guideline aims is to strengthen the regulations and supervision of non-cash, digital payments in the industry.

Improve the security, and governance of payment gateways, wallets, and other digital payment transactions.

- The guideline aims is to strengthen the regulations and supervision of non-cash, digital payments in the industry.
- Improve the security, and governance of payment gateways, wallets, and other digital payment transactions.
- Aims to ensure regulated entities prioritize and focus on the quality of governance, risk management, and internal security controls for building a safer digital payment environment.
- Strengthen and improve the internal grievance redress mechanism with enhanced disclosures on customer complaints.
- Effective implementation and monitoring of certain minimum standards on security controls.
- Overall, aim is to ensure secure online payment transactions and prevent incidents of a data breach, theft, or data leakage of sensitive customer information.

Key Areas Covered in the RBI's Master Direction

The Master Direction is a detailed 21-page dossier issued by the RBI which specifies security protocols to be implemented in mobile applica-

The Master Direction is a detailed 21-page dossier issued by the RBI which specifies security protocols to be implemented in mobile applications, internet banking, and card payments by scheduled commercial banks, small financial and payment banks, and card issuing institutes. The guide line includes specifications on diverse areas, including important Security Controls concerning:-

- Governance and Management of Security Risks
- Generic Security Controls
- Application Security Life Cycle (ASLC)
- Authentication Framework
- Fraud Risk Management,
- Reconciliation Mechanism
- Customer Protection
- Awareness and Grievance Redressal Mechanism related to Internet Banking, Mobile Payments Application Security Controls, and Card Payments Security.
- Special emphasis on following various Payment Card Security Standards as per Payment Card Industry (PCI).

RBI aims to push the regulated financial institutes and NBFC’s to improve the overall operations, security controls and customer care services.

» Digital Payment Security Controls In A Glance

Digital Payment Security Controls

CHAPTER II

Governance & Management of Security Risks

Policy for Digital Payment Products & Services	Risk Management & Governance Program	Controls for Monitoring the Activities of the Third Party	Risk Assessment	Capacity Management Plan	Data Recovery System & Procedure

Generic Security Controls

Communication Protocols	Storage of Sensitive Data	Implementation of Firewalls & DDoS Protection	Renewal of Digital Certificates	Logging and Monitoring Activities

Application Security Lifecycle

Multi-tier Application Architecture	Threat Modeling Approach	Security Testing	Activity Monitoring Mechanism	Security Controls for Digital Payment Applications

Authentication Framework

Multi-factor Authentication	Authentication Attempts

System Fraud Management

System Alerts	Fraud Analysis Mechanism	Train Staff	Incident Response

Reconciliation Mechanism

Real-time reconciliation Mechanism

Customer Protection, Awareness, Grievance Redressal Mechanism

Usage Guidelines & Training Material	Update & Educate Customers	Mechanism for Consumer Grievance & Redressal	Mechanism for Alerts & Notification

CHAPTER III

Internet Banking Security Controls

Secure internet banking website	System Time-outs	Password Generation

CHAPTER IV

Mobile Application Security Controls

Mechanism for Reinstalling and Verifying Mobile Application	Controls for Mobile Applications	Device Binding	Authentication & Re-authentication Mechanism	Storage of Sensitive Data	Security considerations

CHAPTER V

Card Payment Security

Follow PCI Standards	PCI P2PE Certified Terminal Installation	Secure Card Payment Infrastructure	Security Controls at HSM	Security Controls at ATM's	Robust Surveillance/ Monitoring of Card Transactions	Transaction Limits	Card Data Scanning Tools

CHAPTER II

Governance & Management of Security Risk

1. Policy for Digital Payment Products & Services -

The regulated entity is expected to have in place a comprehensive policy for the Digital Payment Products & Services approved by the Board of Directors and the Senior Management. The policy should explicitly contain payment security requirements covering the areas of functionality, security & performance of products and services. This would include having in place-

- **Controls to protect the confidentiality of customer, data integrity of data and processes associated with the digital product/ services.**
- **Availability of requisite infrastructure.**
- **Payment products built securely offering robust performance, safety, and consistency.**
- **Process for capacity building and expansion with scalability.**
- **Minimal customer service disruption with high availability of systems/ channels.**
- **Efficient and effective dispute resolution mechanism and handling of customer grievance.**
- **Adequate and appropriate review mechanism followed by swift corrective action.**
- **Mechanism for conducting User Acceptance Tests (UAT) in multiple stages before roll out, sign off from multiple stakeholders.**

2. Risk management & Governance Program - Establish a robust Governance and Risk Management program for identifying, analyzing, monitoring, and managing the specific risks. This would include having in place

- **Compliance risk and Fraud risk assessment program.**
- **Performance monitoring systems**
- **Key performance indicators for assessing operational and security norms**
- **Quantitative benchmarks for evaluating the effectiveness of security built.**

3. Controls for Monitoring the Activities of the Third Party - Regulated Entities who are dependent on third party service providers must have in place adequate measures to oversee and controls for monitoring the activities of the third party personnel. The entities shall implement necessary measures in line with RBI guidelines on outsourcing to the third-party.

4. Risk Assessment - The Regulated entities are required to perform Risk Assessment at regular intervals to ensure safety and security of digital payment products and associated processes and services. This is to ensure entities protect the integrity, confidentiality and security of the payment data and evaluate the resilience of their systems. They are also required to maintain database of all systems and applications stor-

ing customer data in the payment ecosystem and ensure compliance with applicable PCI standards in each of the systems.

5. Capacity Management Plan - Entities must have in place appropriate Capacity Management Plan to ensure the established digital payment infrastructure is robust, scalable and resilient to meet the growing demands.

6. Data Recovery System & Procedure - Entities should have procedures to periodically test systems and applications that account data back-ups, and recovery pertaining to digital products and services to ensure there is no loss of transactions or audit-trails.

Generic Security Controls

1. Communication Protocols - Entities should adhere to a secure standards and implement appropriate level of encryption and security.

2. Storage of Sensitive Data - Web applications providing the digital payment products and services should not store sensitive information to prevent compromise in the integrity of the data.

3. Implementation of Firewalls & DDoS Protection - Regulated Entities are required to implement Web Application Firewall (WAF) and DDoS mitigation techniques to secure the digital payment products and services.

4. Renewal of Digital Certificates - Digital certificates used in the ecosystem should be renewed on time by the Regulated Entities.

5. Logging and Monitoring Activities - Mobile Application and Internet Banking Application should have effective logging and monitoring capabilities to track user activity, security changes and identify anomalous behavior and transactions.

Application Security Lifecycle

1. Multi-tier Application Architecture - Entities must implement a multi-tier application architecture, segregating application, database and presentation layer adopting a secure by design practice for developing digital payment products and services.

2. Threat Modeling Approach - The Regulated entities must adopt and incorporate a threat modelling approach into their policies, processes, guidelines and procedures during the course of Application Lifecycle Management.

3. Security Testing - Entities must conduct various security testing including review of source code, Vulnerability Assessment (VA) and Penetration Testing (PT) of their digital payment applications at a regular interval to ensure that the application is secure.

4. Activity Monitoring Mechanism - Entities must implement a mechanism to actively monitor non-genuine/ unauthorized/ malicious Payment Applications on app stores and webs and respond accordingly to bring them down.

5. Security controls for Digital Payment Applications - Considering various OWASP standards, security and data protection guidelines in ISO 12812, threat catalogues and guides developed by NIST, entities must accordingly deploy the best Security controls for digital payment applications.

Authentication Framework

1. Multi-factor Authentication - Entities should implement multi-factor authentication for payment through electronic modes and fund transfers.

2. Authentication Attempts - Regulated Entities should set maximum number of failed log-in or authentication attempts after which access to the digital payment product/ service shall be blocked.

Fraud Risk Management

1. System Alerts - Entities must have in place parameterized and monitored alert systems to alert the customers in case of failed authentication, fund transfers, cash withdrawals, payments through electronic modes, adding new beneficiaries etc.

2. Fraud Analysis Mechanism - Fraud analysis mechanism must be in place to identify fraud occurrence and determine mechanism to prevent such frauds.

3. Train staff - Regular training should be provided to staff in the fraud control function to educate and train them with skills and areas of expertise in-

- Fraud control tools and their usage;
- Investigative techniques and procedures;
- Cardholder and merchant education techniques to prevent fraud;
- Scheme/ Card operating regulations;
- Data processing and analysis and liaising or communicating with law enforcement agencies;

4. Incident Response - Regulated Entities must have in place mechanism for handling and responding to Incidents related to payment ecosystem and mitigate the loss either to the customer or Regulated Entities.

Reconciliation Mechanism

1. Real-time Reconciliation Mechanism - Regulated Entities must establish an effective, real-time reconciliation mechanism (not later than 24 hours from the time of receipt of settlement file(s)) for all digital payment transactions between the Regulated Entities all other stakeholders such as payment system operators, business correspondents, card networks, payment system processors, payment aggregators, payment gateways, third party technology service providers, other participants, etc. This is for better detection and prevention of suspicious transactions.

Customer Protection, Awareness and Grievance Redressal Mechanism

1. Usage Guidelines & Training Material - Regulated Entities must provide usage guidelines and training materials for end users and make it mandatory for users to go through secure guidelines.

2. Update and Educate Customers - Regulated entities must educate customers and keep them updated about the best usage practice of digital payment applications.

3. Mechanism for Consumer Grievance & Redressal - Entities are expected to have in place an effective mechanism for addressing consumer grievance & redressal. This should include clearly specifying the respond timelines, process and procedure (with forms/ contact information, etc.) to lodge consumer grievances and a mechanism to keep this information periodically updated.

4. Mechanism for Alerts & Notification - Entities must establish a mechanism for sending out immediate alerts and notification of fraudulent transactions for instant reporting to the corresponding beneficiary/ counterparty's Regulated Entities. This is to accelerate early detection and quickly trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.

CHAPTER III

Internet Banking Security Controls

1. Secure Internet Banking Websites - Entitles must ensure securing the internet banking websites against authentication-related attacks such as the DOS and brute force attacks by implement additional levels of authentication such as adaptive authentication, strong CAPTCHA (preferably with anti-bot features) with server-side validation, etc. Further, measures to be taken to prevent DNS cache poisoning attacks and for secure handling of cookies.

2. System Time-outs - Establish a mechanism of automated time-out of a sessions after a fixed period of inactivity.

3. Password Generation - Entities must ensure secure generation and dispatching of sensitive passwords with validity for a limited period from the date and time of its creation.

CHAPTER IV

Mobile Application Security Controls

1. Mechanism for Reinstalling and Verifying Mobile Application - In case of detection of any anomalies or exceptions for which the mobile application was not programmed, there should be a process in place that reinstall a new version and verify the before the transactions are enabled.

2. Controls for Mobile Applications - Entities must implement the below mentioned controls for their mobile applications -

- Device policy enforcement;
- Application secure download/ install;
- Deactivating older application versions in a phased but time bound manner and maintain only one version of the mobile application on a platform/ operating system;
- Storage of Customer Data;
- Device or Application Encryption;
- Ensuring minimal data collection/ app permissions;
- Application sandbox/ containerisation;
- Identify remote access applications and prohibit login access to the mobile application, as a matter of precaution;
- Code obfuscation.

3. Device Binding - Regulated Entities shall ensure Device Binding of Mobile Applications.

4. Authentication & Re-authentication Mechanism - Regulated Entities must have in place appropriate authentication and re-authentication mechanism. This would include -

- An alternatives to SMS-based OTP;
- Re-authentication for when the device or application remains unused for a designated period
- Authentication/ checks/ measures to identify new network connections or connections from unsecured networks like unsecured Wi-Fi connections.

5. Storage of Sensitive Data - Mobile Application should not store/ retain sensitive personal/ consumer authentication information such as user IDs, passwords, keys, hashes, hard coded references on the device and the application should securely wipe any sensitive customer information from memory when the customer/ user exits the application.

6. Security considerations - Entities must design anti-malware capabilities and secure the mobile application against vulnerabilities like SQL injection.

CHAPTER V

Card Payment Security

1. Follow PCI Standards - Regulated Entities are expected to follow various PCI Standards applicable to them which includes -

- **PCI-PIN** (secure management, processing, and transmission of personal identification number (PIN) data);

- **PCI-PIN** (secure management, processing, and transmission of personal identification number (PIN) data);

- **PCI-PTS** (security approval framework addresses the logical and/ or physical protection of cardholder and other sensitive data at point of interaction (POI) devices and hardware security modules (HSMs);

- **PCI-HSM** (securing cardholder-authentication applications and processes including key generation, key injection, PIN verification, secure encryption algorithm, etc.); and

- **PCI-P2PE** (security standard that requires payment card information to be encrypted instantly upon its initial swipe and then securely transferred directly to the payment processor).

2. PCI P2PE Certified Terminal Installation - Entities should install terminals at merchant sites that are PCI P2PE certified.

3. Secure Card Payment Infrastructure - Acquirers shall secure their card payment infrastructure with Unique Key Per Terminal (UKPT) or Derived Unique Key Per Transaction (DUKPT)/ Terminal Line Encryption (TLE).

4. Security Controls at HSM - The Security Controls expected to be implemented at HSM include -

- Log Management
- Access Control Management
- Secure Key Management.

5. Security Controls at ATM's - The Security Controls expected to be implemented at ATM's include –

- BIOS password
- Latest Patches of Operating System
- Anti-Skimming & Whitelisting Solution

6. Robust Surveillance/ Monitoring of Card Transactions-

Entities must institute a mechanism to monitor breaches, if any, on a 24x7 basis, including weekends, long holidays and have in place a robust incident response mechanism to mitigate the fraud loss, on account of suspicious transactions.

7. Transaction Limits -

Entities must have in place transaction limits for domestic and international transactions at Card, BIN as well as at the Regulated Entities levels, set at the card network switch itself.

8. Card Data Scanning Tools –

Entities must adopt card data scanning tools to identify unencrypted payments card data in their ecosystem and adhere the following safety measures -

- Test tools to understand the scope, impact and its capabilities in a test environment.
- Scan tools should be installed in the Regulated Entities premises and devices.
- Card data scanning should not be done remotely.
- Exportable card data must be appropriately masked.
- No data, which is even masked, must be taken out of the RE's premises/ infrastructure.
- Limited access to service providers to conduct the scan or analyze the data or provide only on entities device.

Going Ahead with the Master Direction

Plan of Action for Businesses -

- Businesses should initially conduct a basic assessment of their Digital Payment Ecosystem to understand where they stand with their existing Compliance Program in place.
- The key to achieving Compliance is understanding your Digital Payment Ecosystem and accordingly establishing security measures aligning with the new Master Direction.
- Again, for those businesses that are compliant to some or most of the international standards like PCI, NIST, ISO, OWASP, etc should map their Compliance Program with the RBI's Master Direction to determine the GAP areas.
- For your business to stay ahead in the industry, understanding the law is crucial
- Gaining such insight will help you design a compliance program that aligns well with your business and compliance goals, making the road ahead for Compliance more achievable.
- Preparing ahead of the time before the new master direction comes into effect will save you from the last minute hassle. The earlier your business takes steps towards initiating the Digital Payment Security Program, your business will be in a far better position to deal with the regulation when it comes into effect.
- We also recommend businesses to approach an experienced Cyber Security Consulting firm for assisting you in navigating through the process.
- Consulting an expert from the industry will help your business make an informed decision when designing a Digital Payment Security Program.

About Us

VISTA InfoSec is a Global Cyber Security Consulting firm offering exceptional Cyber Security Consulting & Audit Service, Regulatory & Compliance Consulting Services and Infrastructure Advisory Solutions. With strong industrial presence since 2004, we have been serving clients from across the world with our robust, end-to-end security services and solutions. We are a 100% vendor neutral company with strict no outsourcing policy and built on our core values of strict code of ethics, transparency and professionalism.

OUR SERVICES OFFERINGS

Compliance & Governance

- SOC 1 Consulting & Audit
- SOC 2 Consulting & Audit
- PCI DSS Advisory and Certification
- PCI PIN Advisory and Certification
- PA SSF Advisory and Certification
- ISO 27001 Advisory and Certification
- ISO 20000 Advisory and Certification
- Business Continuity Management (ISO22301)
- Cloud Risk CCM / CStar / ISO27017
- Information Security Audit
- Software License Audit
- ATM Security Assessment

Technical Assessment

- Vulnerability Assessment
- Penetration Testing
- Web App Security Assessment
- Mobile Security Assessment
- Thick Client Application Security Assessment
- Virtualization Risk Assessment
- Secure Configuration Assessment
- Source Code Review

Regulatory And Compliance

- GDPR Consulting and Audit
- HIPAA Consulting and Audit
- CCPA Consulting and Audit
- NESA Consulting and Audit
- MAS-TRM Consulting and Audit
- NCA ECC Compliance
- SAMA Compliance

Managed Service

- Adaptive Security Managment Pro gram
- DPO Consultancy Services
- CISO Advisory
- Managed Compliance Services
- Managed Security Services

IT Audit & Advisory

- Infrastructure Audit
- Infrastructure Design & Advisory
- Datacenter Design & Consultancy Services

Training & Skill Development

- Training & Skill Development

OUR OFFICES

USA

📍

VISTA INFOSEC LLC
24007 VENTURA BLVD
SUITE 285
CALABASAS CA 91302

☎

+1-415-513-5261

✉

USSALES@VISTAINFOSEC.COM

SINGAPORE

📍

VISTA INFOS EC PTE. LTD
20 COLLYER QUAY
#09-01
20 COLLYER QUAY
SINGAPORE (049319)

☎

+65-3129-0397

✉

SGSALES@VISTAINFOSEC.COM

INDIA

📍

VISTA INFOSEC PVT. LTD
001, NORTH WING,
2ND FLOOR,
NEOSHINE HOUSE,
LINK ROAD, ANDHERI (W)
MUMBAI - 400053

☎

+91 99872 44769
+91-22-26300683

✉

SALES@VISTAINFOSEC.COM

UK

📍

6 AMBER COURT
GOLDSMITH CLOSE
HARROW, GREATER LONDON
UNITED KINGDOM
HA20EZ

☎

+447405816761

✉

UKSALES@VISTAINFOSEC.COM

Webinar : RBI’s Master Direction on Digital Payment Security Controls

CONTACT US

VISTA INFOSEC®
TRUSTED ADVISORS, ASSURED COMPLIANCE™

☎ US Tel: +1-415-513-5261 | SG Tel: +65-3129-0397 | IN Tel: +91 73045 57744

W: www.vistainfosec.com | E: info@vistainfosec.com

You can reach us on