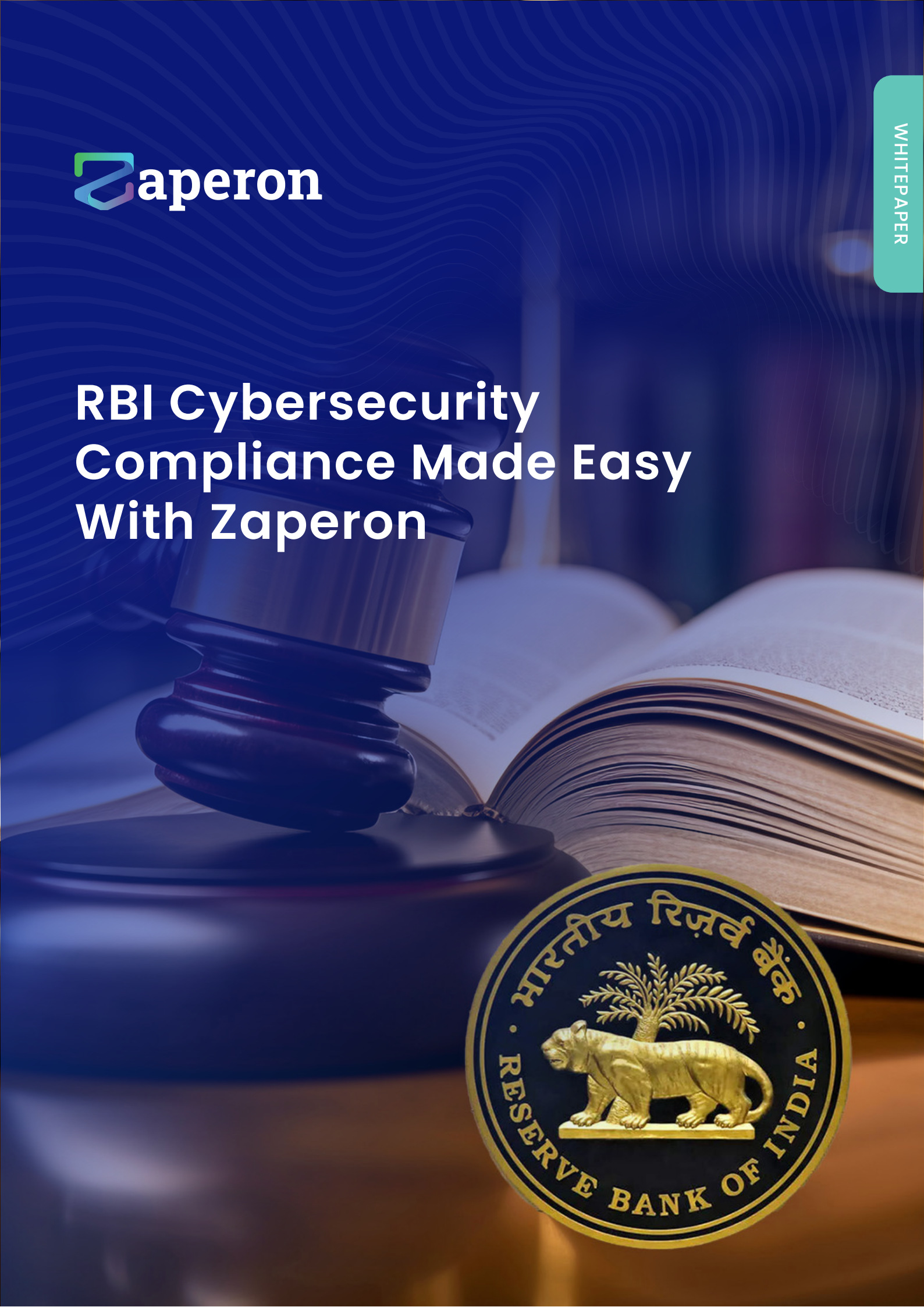
Zaperon

WHITEPAPER

RBI Cybersecurity Compliance Made Easy With Zaperon



Introduction

The **Reserve Bank of India (RBI)**, as the central banking institution of India, plays a crucial role in overseeing the country's financial system. RBI's stringent stance on cybersecurity stems from the need to protect the financial sector from increasingly sophisticated cyber threats. With the rapid digitalization of banking services, the risk of cyberattacks has grown exponentially, making it imperative for the RBI to enforce robust cybersecurity measures.

According to the IBM Cost of a Data Breach Report 2023, the financial sector ranks second globally in terms of cyber incident damage. Financial organizations faced losses averaging approximately **$5.9 million per cyberattack**.

Based on threat intelligence regarding potential cyberattacks, RBI in June 2024 issued a warning to its regulated entities to implement safeguards against these threats. They have also been advised to constantly monitor their systems like SWIFT, the card network, RTGS, NEFT and UPI.

By mandating compliance with robust security standards, conducting regular audits, and promoting data privacy, RBI safeguards the integrity of the financial system. These efforts not only mitigate risks and ensure business continuity but also bolster trust among customers and uphold India's financial stability amidst global cybersecurity challenges.



New IT Governance and Cybersecurity Rules for Financial Entities by RBI

On **November 7, 2023**, the RBI issued a Master Direction on Information Technology DoS.CO.CSITEG/SEC.7/31.01.015/2023-24

This directive came into effect from April 1, 2024, and it applies to regulated entities (REs), which include both banking and non-banking financial companies.

The directive aims to enhance cybersecurity measures and ensure compliance with robust IT standards across the financial sector.

1. **IT Governance Framework:** Regulated Entities (REs) must establish an IT Governance Framework that is required to ensure accountability and mitigate information security risks.
2. **IT and Information Security Risk Management Framework:** REs are required to implement a comprehensive risk management framework that should identify, assess, manage, and monitor risks associated with IT and information security.
3. **Information Security Policy and Cyber Security Policy:** The directive mandates that REs develop and maintain both an Information Security Policy and a Cyber Security Policy. These policies should outline the organization's approach to managing and securing its information and cyber resources.
4. **Periodic Review of IT-Related Risks:** REs are required to perform regular reviews of their IT-related risks. This ensures that any emerging threats or vulnerabilities are identified and addressed promptly.

Who Needs to Comply?

- Banks (Public, Private, Cooperative)
- Non-Banking Financial Companies (NBFCs)
- Payment System Operators
- Authorized & Primary Dealers
- Money Transfer Service Providers
- Credit Information Companies
- Housing Finance Companies
- Asset Reconstruction Companies

Consequences of Non-Compliance

FINANCIAL PENALTIES
Fines imposed by RBI

REPUTATIONAL DAMAGE
Tarnished reputation and lost trust

LEGAL CONSEQUENCES
Risk of litigation and criminal charges

ADMINISTRATIVE ACTIONS
Possible suspension or license revocation

OPERATIONAL RESTRICTIONS
Limitations on business activities

INCREASED REGULATORY SCRUTINY
More frequent audits

RBI fined AP Mahesh Cooperative Urban Bank **₹65 lakhs** for IT governance lapses and cybersecurity framework violations after a ₹12.48 Crore cyber theft in January 2022.

महेश बैंक ®
ESTD. 1978

Union Bank of India

RBI levied a penalty of **₹1 crore** on Union Bank of India for inadequate measures to prevent cyber threats that resulted in fraud transactions worth $171 Million through SWIFT system of the bank

Ensure RBI Compliance with Zaperon's Identity Protection Platform 2.0

SECTION 15

AUDIT TRAILS

(a) Every IT application which can access or affect critical or sensitive information, shall have necessary audit and system logging capability and should provide audit trails.

(b) The audit trails shall satisfy a RE's business requirements apart from regulatory and legal requirements. The audit trails must be detailed enough to facilitate the conduct of audit, serve as forensic evidence when required and assist in dispute resolution, including for non-repudiation purposes.

(c) REs shall put in place a system for regularly monitoring the audit trails and system logs to detect any unauthorized activity.

COMPLY WITH ZAPERON

Zaperon provides logs of all applications accessed by the users and security posture of the devices, and gives visibility in the form of dashboards. Activities of the admin users can also be tracked in the system logs.

SECTION 16

CRYPTOGRAPHIC CONTROLS

The key length, algorithms, cipher suites and applicable protocols used in transmission channels, processing of data and authentication purpose shall be strong. REs shall adopt internationally accepted and published standards that are not deprecated/ demonstrated to be insecure/ vulnerable and the configurations involved in implementing such controls shall be compliant with extant laws and regulatory instructions.

COMPLY WITH ZAPERON

Zaperon employs Public Key Infrastructure (PKI) in Identity Protection 2.0 for enhanced security and streamlined authentication. Zaperon generates a unique PKI certificate for each end-user device, enabling passwordless single sign-on, certificate-based authentication and Zero Trust Access control, safeguarding enterprise applications and networks.

SECTION 19a

ACCESS CONTROLS

Access to information assets shall be allowed only where a valid business need exists. REs shall have documented standards and procedures, which are approved by the ITSC and kept up to date for administering need-based access to an information system.

SECTION 19b

Personnel with elevated system access entitlements shall be closely supervised with all their systems activities logged and periodically reviewed.

COMPLY WITH ZAPERON

Granular access controls can be imposed in Zaperon by enforcing policies based on the user's role, device identity, IP, geo-location, anti-virus, operating system version, and access time. Zaperon implements role-based access control (RBAC) and least privilege access, ensuring that users are only granted access to enterprise resources and data as per their assigned privileges. They also get access only from authorized and secure devices. Continuous monitoring is done to ensure compliance with access policies. Activities of the privileged users in Zaperon management console are logged for audit purposes.

SECTION 19c

REs shall adopt multi-factor authentication for privileged users of **i)** critical information systems and **ii)** for critical activities, basis the RE's risk assessment.

COMPLY WITH ZAPERON

For all critical systems, Zaperon uses strong authentication using PKI and phishing-resistant MFA (Multi-Factor Authentication), validating 15+ factors related to certificate, user behavior and device posture.

SECTION 20

CONTROLS ON TELEWORKING

In the teleworking environment, REs, inter alia, shall:

(a) Ensure that the systems used and the remote access from alternate work location to the environment hosting RE's information assets are secure;

(b) Implement multi-factor authentication for enterprise access (logical) to critical systems;

(c) Put in place a mechanism to identify all remote-access devices attached/ connected to the RE's systems; and

(d) Ensure that data/ information shared/ presented in teleworking is secured appropriately.

COMPLY WITH ZAPERON

Zaperon, with its zero trust architecture, secures remote workers' access to apps, network devices, and servers without the need for a VPN that has vulnerabilities. Implementing phishing-resistant multi-factor authentication (MFA) provides robust protection for critical systems. Additionally, Zaperon logs the posture of all the devices in the network, including those used for remote access. Continuous monitoring of these devices ensures that only secure and compliant devices connect to enterprise resources.



Zaperon Identity Protection 2.0

PKI-BASED PASSWORDLESS AUTHENTICATION

Utilises PKI for secure, passwordless access, reducing the risk of data breaches due to credential compromise.

PHISHING-RESISTANT MULTI-FACTOR AUTHENTICATION

Implements MFA resistant to phishing, enhancing security through 15+ factors.

CONTINUOUS ZERO TRUST ACCESS CONTROL

Enforces zero trust policies continuously based on user behavior and device posture, ensuring compliance and security.

PROACTIVE IDENTITY THREAT DETECTION AND RESPONSE

Detects anomalies and responds to identity threats proactively, mitigating potential security incidents.

COMPREHENSIVE IDENTITY PROTECTION

The comprehensive identity protection with proactive threat detection and response, ensures robust security across users, devices, applications, and cloud infrastructure.

Zaperon redefines identity protection with its advanced platform, safeguarding organizations against identity-based attacks. Utilizing PKI-based passwordless access and phishing-resistant multi-factor authentication, it enforces continuous zero-trust policies based on user behavior and device posture. With proactive identity threat detection and response, Zaperon ensures robust security across users, devices, applications, and cloud infrastructure.

+1 202 600 5234
+91 8800 170387
sales@zaperon.com
www.zaperon.com
© 2024 Zaperon, Inc.
All Rights Reserved.