SECUREYES
Infusing Security

Simplifying RBI's CyberSecurity Mandates

for Banking Institutions in India

www.secureyes.net

hello@secureyes.net

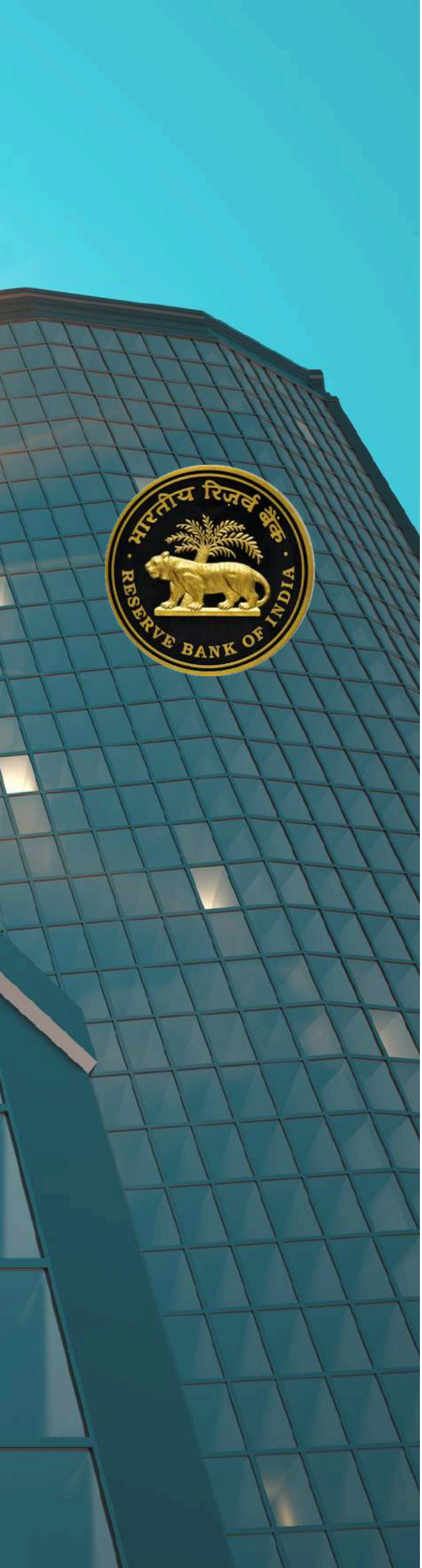
This document serves as a comprehensive resource for:

- **CISOs,**
- **CCOs,**
- **CROs,**
- **IT-Heads,**
- **CTOs, and**
- **Heads-GRCs**

of Indian Banks to understand and implement the RBI's cybersecurity and third-party risk management mandates.

✅✅✅

By adhering to these guidelines, banks can significantly enhance their cybersecurity posture, ensure regulatory compliance, and build a resilient financial ecosystem. Proactive measures and continuous improvement in cybersecurity practices will not only protect the banks but also foster trust and confidence among customers and stakeholders.



CONTEXT

Stable

The Reserve Bank of India (RBI) is the central banking institution of India, responsible for the regulation and supervision of the financial system. It plays a pivotal role in ensuring the stability and integrity of the banking sector.

Secure

In an era where cyber threats are increasingly sophisticated and pervasive, the RBI has issued comprehensive **guidelines to help banks fortify their cybersecurity frameworks and manage third-party risks effectively**.

Financial System

Adhering to the RBI's cybersecurity guidelines is not just a regulatory requirement but a critical component of a bank's risk management strategy. Non-compliance can lead to severe financial penalties, reputational damage, and loss of customer trust.

More importantly, robust cybersecurity measures are essential to protect sensitive customer data, maintain operational continuity, and safeguard the financial system's integrity.

RBI Kehta Hai...
Jaankar Baniye,
Satark Rahiye!

SecurEyes
Infusing Security

PROACTIVE CYBERSECURITY MEASURES

Being proactive in addressing cybersecurity offers numerous benefits:

ENHANCED SECURITY POSTURE

Proactive measures help in identifying and mitigating vulnerabilities before they can be exploited.

REGULATORY COMPLIANCE

Adherence to RBI guidelines ensures compliance with regulatory requirements, avoiding penalties and legal repercussions.

CUSTOMER TRUST

Strong cybersecurity measures build customer confidence in the bank's ability to protect their data.

OPERATIONAL RESILIENCE

Effective cybersecurity frameworks ensure business continuity even in the face of cyber incidents.

COMPETITIVE ADVANTAGE

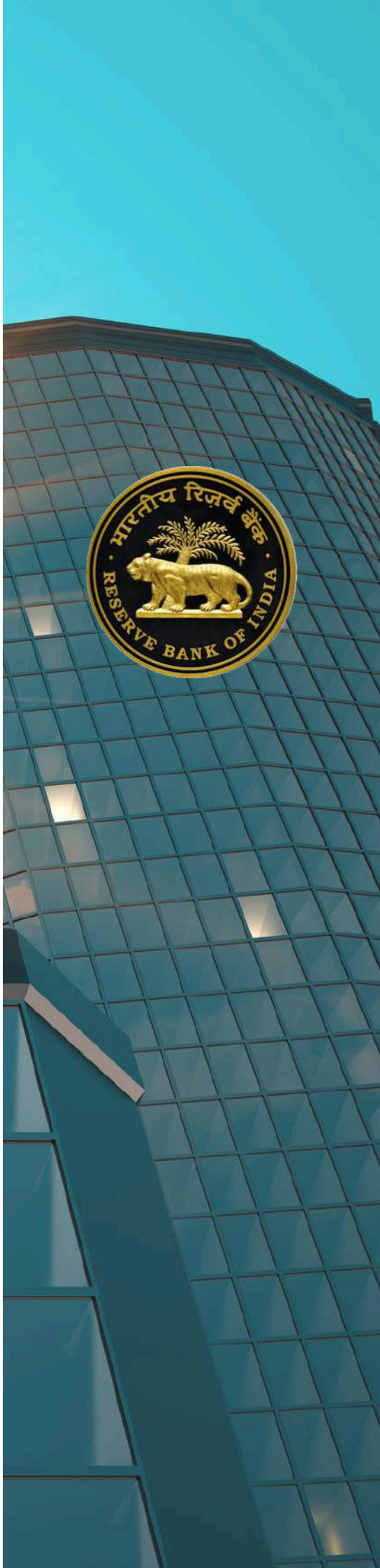
Banks with robust cybersecurity frameworks can differentiate themselves in the market, attracting more customers and partners.

SecurEyes
Infusing Security

RBI MANDATES & GUIDELINES

What's included?

- Cyber Security Framework and Policy
- Baseline Cyber Security and Resilience Requirements
- Cyber Security Operations Centre (C-SOC)
- Cyber Security Incident Reporting (CSIR)
- Third-Party Risk Management (TPRM)
- General Guidelines



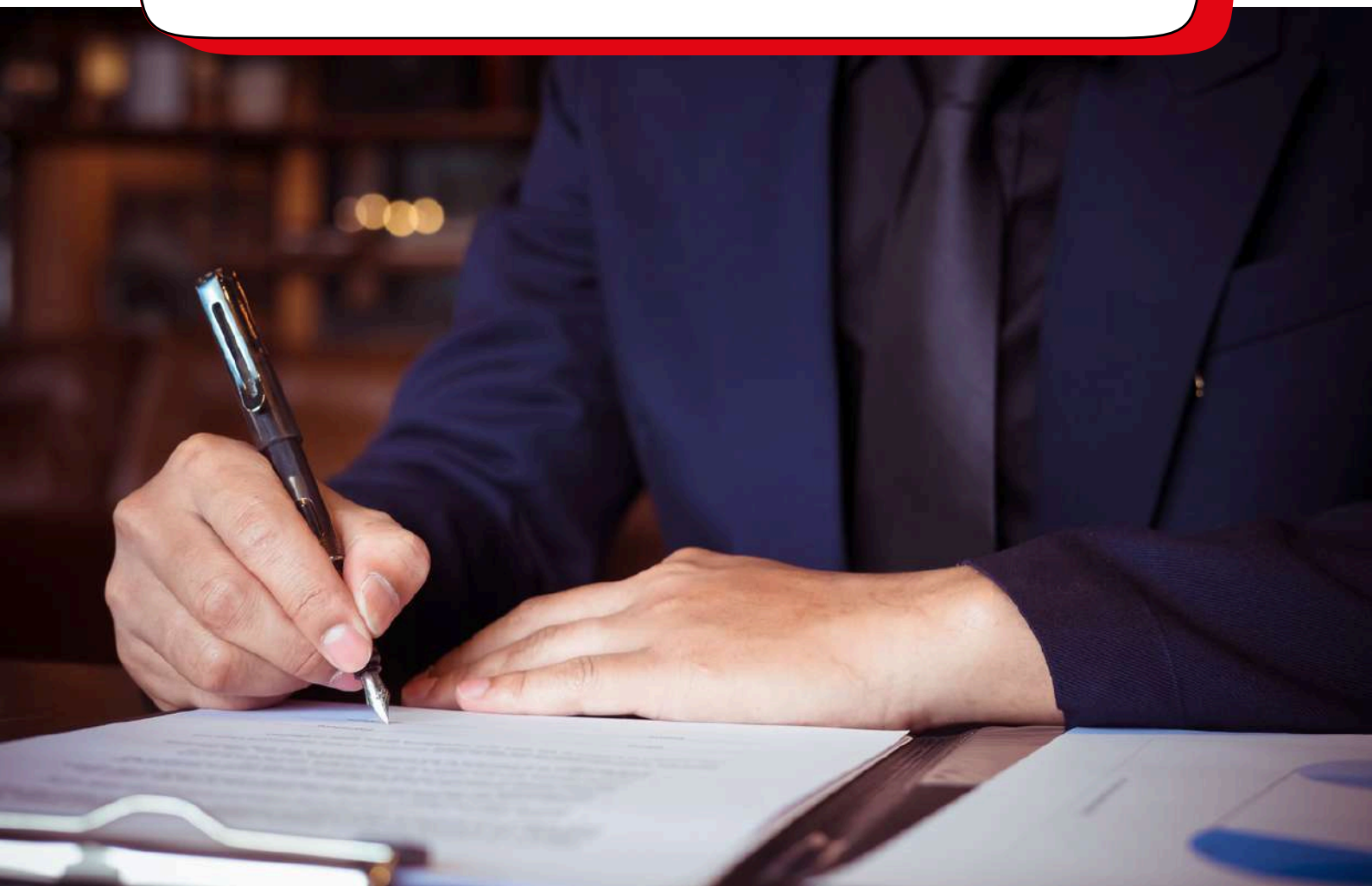
SecurEyes
Infusing Security

RBI
MANDATES & GUIDELINES

CYBER SECURITY FRAMEWORK & POLICY

Key Takeaway:

Banks must establish a robust, board-approved cybersecurity framework that includes risk assessment, continuous monitoring, IT security measures, crisis management, vulnerability testing, and mandatory reporting of cyber incidents to the RBI.



CYBER SECURITY FRAMEWORK & POLICY

01

Cyber Security Policy

Banks must have a Board-approved cyber-security policy distinct from their broader IT or IS security policy. The policy should outline the strategy to combat cyber threats, considering the complexity of the bank's business and acceptable risk levels. It should address cyber risks and mitigation measures.

02

Risk Assessment

Banks must identify inherent risks considering technologies adopted, business and regulatory alignment, connections, delivery channels, online/mobile products, technology services, organizational culture, and internal/external threats. Banks need to categorize their risk levels (low, moderate, high, very high) based on this assessment.

03

Continuous Surveillance

Banks are mandated to set up a Security Operations Center (SOC) for continuous surveillance and to stay updated on emerging cyber threats. The SOC should monitor and manage cyber risks in real-time.

04

IT Architecture

Banks' IT architecture must facilitate security measures. The IT Sub-Committee of the Board should review and upgrade the architecture as per risk assessments.

05

Network and Database Security

Banks need to review network security thoroughly. They must prevent unauthorised access to networks and databases, and any permitted access should be through well-defined processes.

CYBER SECURITY FRAMEWORK & POLICY

06

Cyber Crisis Management Plan (CCMP)

Banks are required to develop and implement a CCMP as part of their overall strategy. This plan should be distinct from traditional BCP/DR arrangements, addressing detection, response, recovery, and containment. The CCMP must be based on guidance from CERT-In, NCIIPC, RBI, and IDRBT.

07

Vulnerability Testing

Periodic vulnerability testing is mandated to identify security flaws in banks' infrastructure and applications.

08

Cybersecurity Preparedness Indicators

Banks need to define indicators to assess their cyber security and resilience framework.

09

Reporting Cyber Incidents

Banks must report all unusual cyber security incidents (successful or attempted) to the RBI.

10

Information Sharing (Recommended)

Banks should actively participate in the CISO forum coordinated by IDRBT and report incidents to IB-CART.

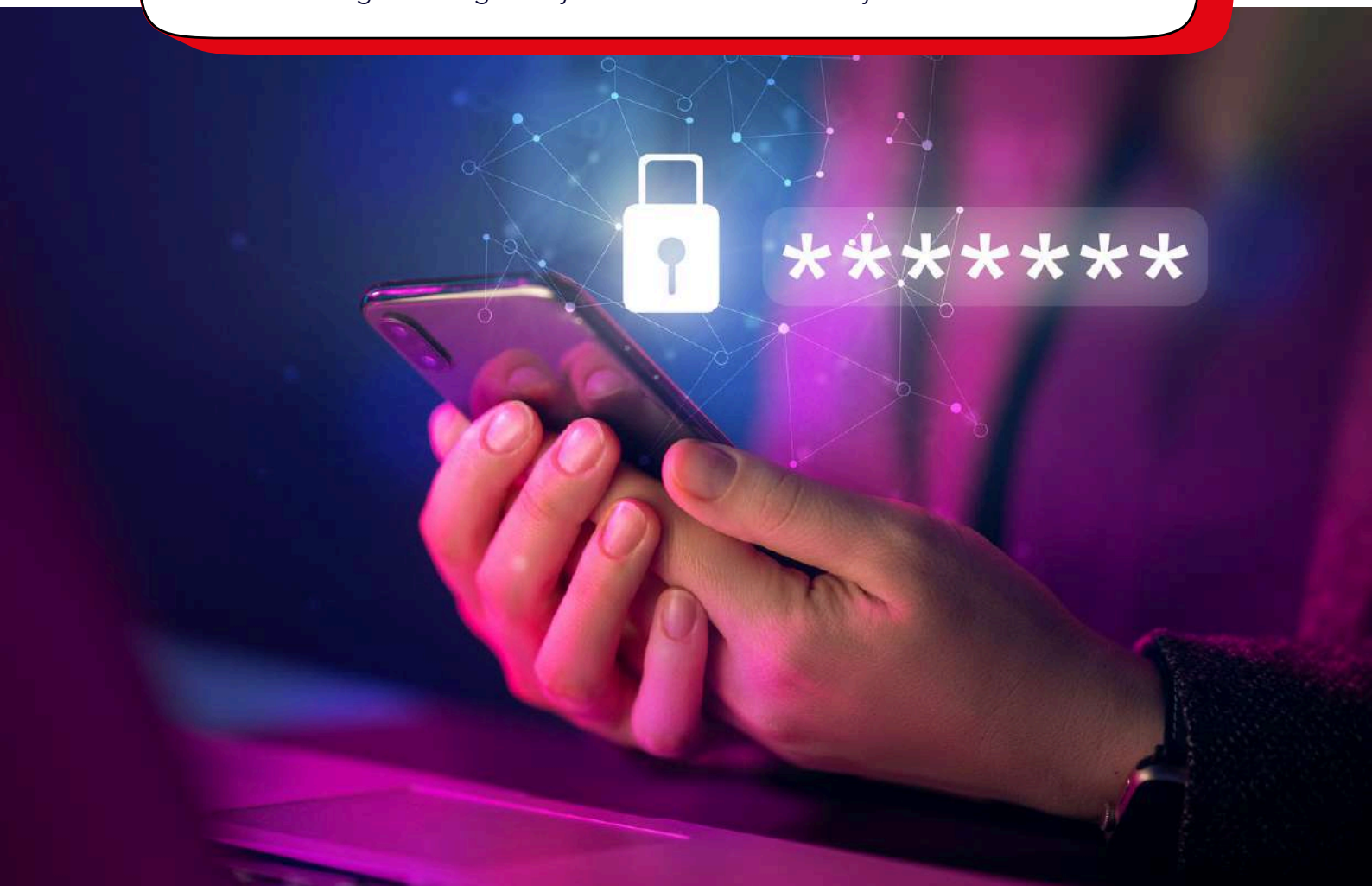
SecurEyes
Infusing Security

RBI MANDATES AND GUIDELINES

BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENTS

Key Takeaway:

Banks must implement baseline cybersecurity and resilience measures, including IT asset management, secure application development, patching, access controls, secure communication, vendor risk management, incident response, and continuous monitoring to mitigate cyber threats effectively.



BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENTS

01

Inventory Management

Banks need to maintain an inventory of business IT assets, classifying them based on business criticality. Data must be classified based on sensitivity.

02

Software Control

Banks need to control the execution of unauthorized software and maintain an inventory of authorized/unauthorized software.

03

Application Security

Secure coding practices and source code audits are required for in-house and collaboratively developed applications.

04

Patch Management

Banks should have systems to identify, track, manage, and monitor the status of patches to operating systems and application software.

05

Network Management

Banks must maintain network architecture diagrams and inventories of authorized devices connected to the network, along with appropriate security configurations.

06

Web Security

Secure web gateways, with features such as deep packet scanning, are to be implemented.

BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENTS

07

User Access Control

Banks need to implement measures for controlling user access, with privileged access managed using the principle of least privilege and separation of duties.

08

Authentication

Banks need to implement a framework for customer authentication.

09

Secure Communication

Banks need secure email and messaging systems to prevent spoofing and malicious links.

10

Vendor Risk Management

Banks are responsible for managing and assuring security risks in outsourced and partner arrangements. RBI should have access to information resources consumed by banks even if the infrastructure isn't physically located in the bank premises. Banks must ensure compliance with legal requirements relating to data location.

11

Removable Media

Banks need policies for secure use of removable media.

12

Anti-phishing

Banks should subscribe to anti-phishing/anti-rouge app services to identify and take down malicious sites/apps.

BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENTS

13

Data Leak Prevention

Banks must have a data loss/leakage prevention strategy.

14

Vulnerability Assessment

Regular vulnerability assessments and penetration testing are needed.

15

Incident Response

Banks must have an effective incident response program.

16

Awareness

Banks need to ensure security policy awareness among users, employees, vendors, and partners.

17

Customer Education (Recommended)

Customer education on cyber risks is important.

18

Risk-based transaction monitoring

Banks must implement risk-based transaction monitoring.

SecurEyes
Infusing Security

RBI
MANDATES & GUIDELINES

CYBER SECURITY OPERATIONS CENTRE (C-SOC)

Key Takeaway:

Banks must establish a Cyber Security Operations Centre (C-SOC) to provide real-time monitoring, threat intelligence, and incident response, ensuring proactive cybersecurity management through governance, integration, and advanced technologies.

CYBER SECURITY OPERATIONS CENTRE (C-SOC)

01

Establishment

Banks must establish and operationalize a C-SOC to monitor and manage cyber risks in real-time.

02

Functionality

The C-SOC must have capabilities for dynamic behaviour analysis, threat intelligence, and counter-response services. It should protect business and customer data, provide real-time security posture information, manage security operations, assess threat intelligence, and preserve evidence.

03

Governance

C-SOC should include top management briefings on threat intelligence, dashboards and oversight, policy and enforcement mechanisms, and stakeholder participation.

04

Integration

The C-SOC should integrate various log types, ticketing/workflow systems, and reporting dashboards.

05

Technology

C-SOC should utilize appropriate technology for proactive monitoring aligned with the bank's risk profile.

06

Process

C-SOC must follow processes for incident management, problem management, vulnerability/patch management, security risk management, and computer forensics.

SecurEyes
Infusing Security

RBI
MANDATES & GUIDELINES

CYBER SECURITY INCIDENT REPORTING (CSIR)

Key Takeaway:

Banks must promptly report cyber incidents to the RBI within 2 to 6 hours using a structured template, ensuring transparency, timely mitigation, and regulatory compliance.

CYBER SECURITY INCIDENT REPORTING (CSIR)

01

Reporting Template

Banks are required to report cyber incidents using a specific template to the RBI.

02

Information Required

Reports should include details of the incident, impact assessment, actions taken, communication methods, root cause analysis, and resolution plans.

03

Timelines

Incidents should be reported within 2 to 6 hours. Updates must be provided if investigations are ongoing or new information has emerged.

04

Cyber Security Incident Reporting Form

The reporting form requires details on contact information, incident type, impact, and status, along with a description of the incident.

SecurEyes
Infusing Security

RBI
MANDATES & GUIDELINES

THIRD-PARTY RISK MANAGEMENT (TPRM)

Key Takeaway:

Banks must establish strong oversight and risk management for third-party vendors, ensuring security, compliance, audit rights, and RBI access to outsourced operations.

SECUREYES
Infusing Security

THIRD-PARTY RISK MANAGEMENT (TPRM)

01

Management Structure

Banks should have a management structure to monitor and control outsourcing activities.

02

Regular Audits

Audits by internal or external auditors are required to assess risk management practices in outsourcing.

03

Financial and Operational Review

Banks must review the service provider's financial and operational conditions annually.

04

Right to Audit

Contracts with service providers must allow the bank to conduct audits and obtain review reports.

THIRD-PARTY RISK MANAGEMENT (TPRM)

05

Risk Assessment

Banks must assess outsourcing risks such as strategic, reputational, compliance, operational, legal, exit strategy, counterparty, country, contractual, access, concentration, and systemic risks.

06

Preservation and Protection of Information

Banks need to ensure the security and confidentiality of customer information when outsourcing, with access on a 'need to know' basis.

07

Business Continuity

Service providers must test their business continuity and recovery plans, with banks conducting joint testing.

08

RBI Access to Information

RBI should have access to all information consumed by banks, even if the infrastructure is not physically located on their premises.

SECUREYES
Infusing Security

RBI MANDATES & GUIDELINES

GENERAL GUIDELINES

Key Takeaway:

Banks must take full accountability for cybersecurity, ensuring data protection, board-level oversight, stakeholder awareness, and proactive identification of security gaps.

GENERAL GUIDELINES

01

Customer Information Security

Banks are responsible for the security of customer information even if it is with customers or third parties.

02

Board and Senior Management Awareness

Banks need to ensure the Board of Directors and Top Management are updated on cyber-security aspects.

03

Awareness and Training

Banks need to conduct awareness and training sessions for all stakeholders, including the board, management, employees, third-party vendors, and customers.

04

Gaps in Preparedness

Banks need to identify and report gaps in cyber security preparedness to the RBI, along with proposed measures, timelines, and risk assessment methods.

SECUREYES
Infusing Security

Your trusted partner for Comprehensive AI-POWERED Cybersecurity Solutions

Consulting & Advisory | Cybersecurity Products | Corporate Training & Upskilling

In today's dynamic digital landscape, where cyber threats evolve by the minute and regulatory demands grow increasingly complex, organizations need more than just technology - they need a partner that delivers holistic, end-to-end cybersecurity solutions.

This is where SecurEyes excels.

For 18 years, SecurEyes has been at the forefront of cybersecurity consulting, advisory, product development, and skill enhancement, empowering organizations to secure their digital assets, achieve compliance, and build a resilient future.

Our Offerings

A Consulting & Advisory Services

Whether you're a CISO, CRO, or Head of GRC, navigating complex regulatory frameworks or mitigating emerging threats is no easy task. Our team of experts offers tailored consulting solutions that help you:

01 Enhance your governance, risk, and compliance (GRC) frameworks

02 Strengthen your security posture with proactive risk management

03 Streamline regulatory reporting to meet evolving global standards

SecurEyes
Infusing Security

Our Offerings

B AI-powered Cybersecurity Products

Simplify your security operations with our cutting-edge, integrated product suite. Designed for CISOs, CROs, CIOs, IT Heads, and Program Managers, our tools help:

01 Centralize risk management with platforms like RegTrac and RiskTrac

02 Mitigate third-party risks with TPTrac

03 Automate vulnerability and compliance tracking with VulTrac and CompTrac

SECUREYES
Infusing Security

Our Offerings

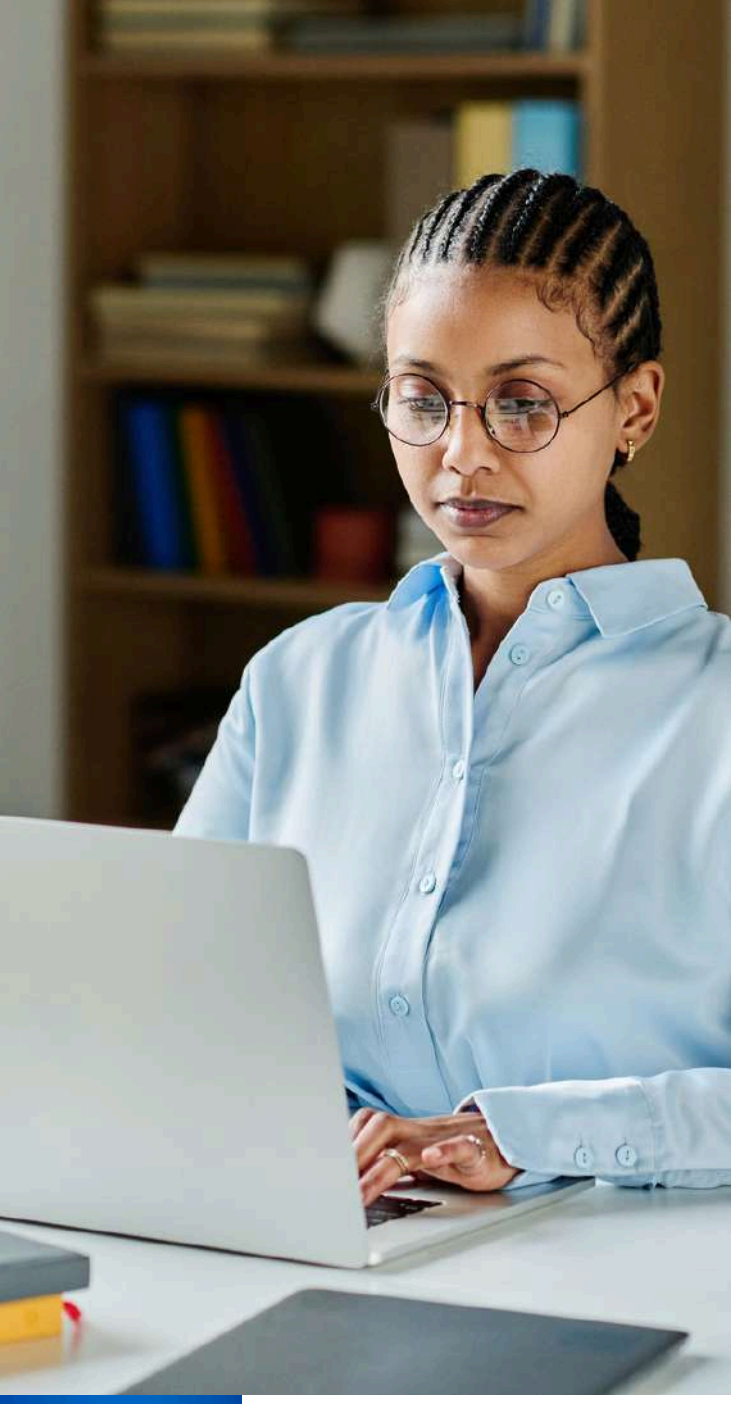
Corporate Training & Upskilling

With human error accounting for over 80% of breaches, building a cyber-aware workforce is crucial. Our tailored training programs for IT teams, compliance officers, and internal auditors:

01 Reduce risk exposure by educating teams on the latest threats

02 Boost incident response times with hands-on workshops

03 Foster a security-first culture across all levels of the organization



SECUREYES
Infusing Security

Our Offerings

D CyberSecurity Certification Program (CSCP)

Our flagship CSCP program is designed for recent graduates, career switchers, and cybersecurity enthusiasts who want to fast-track their careers. In just 3 months, participants gain:

01 Hands-on experience with real-world cybersecurity scenarios

02 Expert mentorship from industry leaders

03 Job placement opportunities at top organizations, including SecurEyes

SECUREYES
Infusing Security

Why Partner with SecurEyes

Proven Expertise: Trusted by Fortune 500 companies, government agencies, and financial institutions worldwide

End-to-End Solutions: From advisory and consulting to products and training, we cover every facet of cybersecurity

Future-Ready Approach: We leverage the latest technologies to help you stay ahead of evolving threats

Customer-Centric Focus: Every solution is tailored to your unique challenges and business goals

By partnering with SecurEyes, you're not just investing in cybersecurity—you're investing in sustainable growth, regulatory confidence, and a resilient digital future.

Let's Explore Synergies

Are you ready to transform your organization's cybersecurity posture?

Let's connect for a 30-minute discussion to explore how SecurEyes can support your journey toward a more secure future.

https://calendly.com/hello-secureyes

www.secureyes.net

hello@secureyes.net

IND +91 9939217654
IND +91 8041264078
UAE +971 50 8950797
USA +1 361 423 1683