Reserve Bank Of India (RBI) Guidelines for Cyber Security Framework

HOW INSTASAFE CAN HELP YOU TO STAY SECURE?

TABLE OF CONTENTS

- Guidelines on Cyber Security Framework — Page 3
- Cyber Security Framework — Page 4
- Annex 1: Baseline Cyber Security and Resilience Requirement — Page 5
- How InstaSafe can help you to comply with baseline Cyber Security and Resilience Requirement — Page 6 - 7
- Annex 2: Setting up and Operationalising Cyber Security Operation Centre (C-SOC) — Page 8
- Annex 3: Template for Reporting Cyber Incidents — Page 8
- About InstaSafe — Page 9

→ GUIDELINES ON CYBER SECURITY FRAMEWORK

With rapid increase in number, frequency, and impact of Cyber incidents/attacks over the last few years, there is urgent need to put in place for a robust cyber security/ resilience framework at enterprises which would provide them with adequate Cyber security preparedness on a continuous basis.

RBI in its circular DBS.CO/CSITE/BC.11/33.01.001/2015-16 provide guidelines for creating robust Cyber security Framework in Banks. It emphasizes the need to move from the present defensive strategy adopted by banks to a more pro-active approach with focus on preventive, detective and corrective cybersecurity controls.

Along with Cyber Security Framework and Guidance, it provides 3 Annexes:
Annex 1: Baseline Cyber Security and Resilience Requirements
Annex 2: Setting up and Operationalizing Cyber Security Operation Centre (C- SOC)
Annex 3: Template for reporting Cyber Incidents

→ CYBER SECURITY FRAMEWORK RECOMMENDED BY RBI

1 Cyber Security Policy	• Need to have Cyber Security Policy which is distinct and separate from broader IT policy /IS security policy • Identify inherent risks and controls in place. • Prevent, detect and take corrective Cyber security controls as per Annex 1
2 IT Architecture	• IT architecture should take of facilitating the security measures to be in place at all times • Needs to be reviewed by IT sub Committee and upgraded as per need. • Proactively initiate Security Operation Centre (SOC) as per Annex 2
3 Network and Database Security	• Thorough review of entire network security • Well defined process to avoid unauthorized access to networks and databases • Responsibility should be clearly defined
4 Customer Information	• Appropriate steps required in preserving the confidentiality, Integrity, and availability of the same. • Suitable measures and process to be put in place
5 Cyber Crisis Management Plan (CCMP)	• CCMP needs to be formulated and part of overall Board approved strategy • CCMP should address the following four aspects – Detection, Response, Recovery and Containment.
6 Preparedness Indicators	• Cyber Security preparedness indicators should be formulated to assess the level of risk/ preparedness. • Awareness to be done for all stakeholders including employees
7 Gap Assessment	• The material gaps in control may be identified early and appropriate remedial action to be initiated. • Identified Gaps, proposed measures, milestones with timelines to be reported to RBI.
8 Reporting Cyber Incidents	• Banks are required to report immediately any cyber incidents to RBI as per format in Annex 3

→ ANNEX 1: BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENT

Baseline Cyber Security and Resilience Requirement

1. Inventory Management of Business IT Assets	2. Preventing Execution of Unauthorized Software	3. Environmental Controls
4. Network Management and Security	5. Secure Configuration	6. Application Security Life Cycle (ASLC)
7. Patch/Vulnerability and Change Management	8. User Access Control/ Management	9. Authentication Framework for Customers
10. Secure Mail and Messaging Systems	11. Vendor Risk Management	12. Removable Media
13. Advanced Real-Time Threat Defense and Management	14. Anti-Phishing	15. Data Leak Prevention Strategy
16. Maintenance, Monitoring and Analysis of Audit Logs	17. Audit Log Settings	18. Vulnerability Assessment and Penetration test and Red Team
19. Incident Response & Management	20. Risk Based Transaction Monitoring	21. Metrics
22. Forensics	23. User/ Employee/ Management Awareness	24. Customer Education and Awareness

Solution Scope of InstaSafe

→ HOW INSTASAFE CAN HELP YOU TO COMPLY WITH BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENT

2 Preventing Execution of Unauthorized Software	• InstaSafe Zero Trust platform can block installation & running of unauthorized software application.
4 Network Management and Security	• InstaSafe Zero Trust platform maintains a list of authorized devices mapped to its users which are authorized to access networks • Any login from new devices is sent to administrator for approval. Administrator can approve or deny the request.
5 Secure Configuration	• InstaSafe Zero Trust platform maintains a list of authorized devices mapped to its users which are authorized to access networks.
6 Application Security Life Cycle (ASLC)	• InstaSafe Zero Trust platform maintains secure coding practices and follows OWASP guidelines for software development
7 Patch/Vulnerability & Change Management	• InstaSafe periodically conducts VA/PT of all its web and mobile applications. Using InstaSafe solution, organizations can push patch updates to employees' machines.
8 User Access Control/ Management	• InstaSafe Zero Trust platform provide secure access to enterprise applications from within/outside enterprise's network. Our multi factor authentication functionality provides enhanced authorization functionality.
9 Authentication Framework for Customers	• InstaSafe Zero Trust platform can integrate with various enterprise directory services such as Azure AD, LDAP, OnPrem AD and others • Supports various Authentication protocols including RADIUS, TACACS, FIDO, and SAML
10 Secure mail and messaging systems	• InstaSafe Zero Trust provides secure access to email and messaging services.

→ HOW INSTASAFE CAN HELP YOU TO COMPLY WITH BASELINE CYBER SECURITY AND RESILIENCE REQUIREMENT:

11 Vendor Risk Management	• InstaSafe provides secure third party access to business applications after strict authentication mechanisms with added MFA . Application specific and time based access is provided with complete monitoring of user activity.
12 Removable Media	• InstaSafe provides USB controls with regard to blocking use of Pen Drive, Hard drive, and Mobile Phone
15 Data Leak Prevention Strategy	• InstaSafe offers various data leak prevention features which include blocking copy/paste, block screen capture, block file download, disable clipboard access, screen recording, Watermark protection and Single device login
16 Maintenance, Monitoring, and Analysis of Audit Logs	• InstaSafe offers detailed reporting of user and network activity with audit logs. It can also be integrated with existing SIEM tool of the organization.
17 Audit Log Settings	• Detailed audit logs are captured with information including user details, login details, device details, IP information, and application accessed details.
18 VA/PT and Red Teaming	• InstaSafe periodically conducts Vulnerability Assessment and Penetration testing both in-house and with external certified agencies. All remediation steps are incorporated during periodic product releases.
19 Incident Response and Management	• InstaSafe has responsible vulnerability disclosure policy where external security researchers can report security bugs and it gets addressed appropriately by security team
23 User / Employee / Management Awareness	• InstaSafe conducts regular cybersecurity training and awareness sessions for internal employees.
24 Customer Education and Awareness	• InstaSafe regularly sends cybersecurity newsletter to all customers to spread awareness and stay updated with cybersecurity trends.

→ ANNEX 2: SETTING UP AND OPERATIONALISING CYBER SECURITY OPERATION CENTRE (C-SOC)

Cyber Security Operations Centre (C-SOC)

1. Governance Issues	2. Technology Issues	3. Process related Issues
4. People related Issues	5. External Integration	6. Incident Management

→ ANNEX 3: TEMPLATE FOR REPORTING CYBER INCIDENTS

Cyber Security Operations Centre (C-SOC)

Security Incident Reporting (SIR) to RBI (within 2 to 6 Hours)
Subsequent update(s) to RBI (updates to be provided if the earlier reporting was incomplete i.e investigation underway or new information pertaining to the incident has been discovered or as per request of RBI)

About InstaSafe

InstaSafe's mission is to secure enterprises from the abuse of excessive trust and privilege access. We empower organizations across to globe in preparing their security infrastructure for digital transformation in a cloud-dominated world. Recognized by Gartner as one of the top representative vendors providing Zero Trust Security, InstaSafe Secure Access, InstaSafe Zero Trust Application Access, and InstaSafe Authenticator follow the vision that trust can never be an entitlement, to offer securely enhanced and rapid access of enterprise applications to users situated anywhere across the globe. We secure 500,000 endpoints for more than 150 customers, spread across 5 continents, with our 100% cloud-delivered solutions, ensuring that our offerings are in line with our mission of being Cloud, Secure, and Instant.

Problems? Talk to us

Let's talk more about how InstaSafe can empower your remote workforce through transformational and seamless security.

sales@instasafe.com

www.instasafe.com

You can connect us at:

/instasafe /instasafe /instasafe /instasafeZT