Roadmap to achieve Comprehensive Cyber Security Framework for Rural Cooperative Banks (RCBs) alignment with NASMS

NASMS alignment with RBI-RCBs Cyber Security Guidelines

Wissen Baum

Preface:

The Rural co-operative banks digitally transforming from Traditional Banking and to the new generation industry by offering state of the art digital products to its customers. This use of Information Technology by banks has grown rapidly and is now an important part of the operational strategy of banks. The number, frequency and impact of cyber incidents/attacks have increased manifold in the recent past, more so in the case of financial sector including banks. RBI has issued the Cyber Security frameworks which focuses on following four areas

1. Cyber Security and Resilience Requirements – Level I
2. Cyber Security and Resilience Requirements – Level II
3. Cyber Security and Resilience Requirements – Level III
4. Cyber Security and Resilience Requirements – Level IV

These guidelines focus on **Cyber Security Policy, IT Architecture and Framework, Cyber Crisis Management Plan, Organisational Arrangements, Cyber Security Awareness, Protection of information, Risk and Gap Assessment, Network Security, Continuous Surveillance and Incident Reporting.**

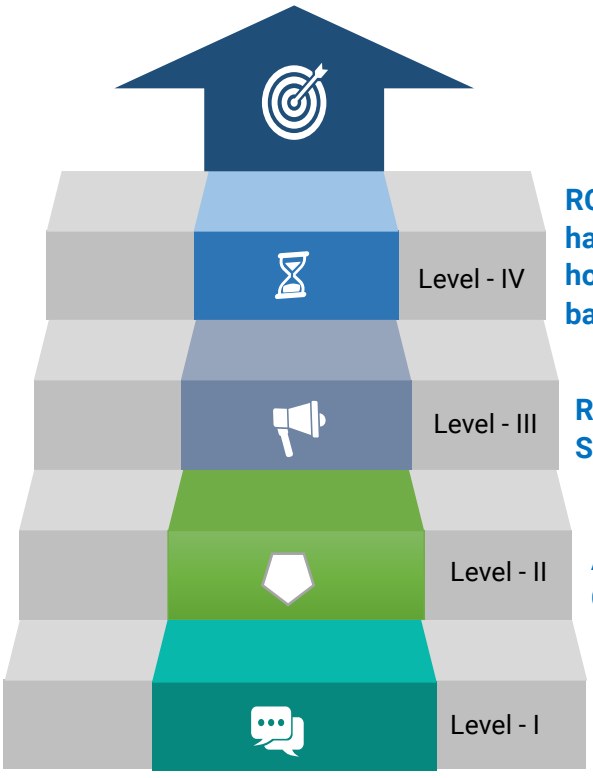
Wissen Baum along with our global partners has developed one stop innovative solution for Asset Life cycle management, Vulnerabilities management, Data and Network Security management for continuous Surveillance and Incident reporting. Our SME support will assist in creating Cyber Security Policy, conduct the Risk and Gap assessment, creating Cyber Crisis Management Plan, creating Cyber Security Awareness which is aligned to RBI's guidelines. This makes you to focus on the key objective of sustainability & growth.

RBI-RCBs

Cyber Security Guidelines

Alignment with NASMS

RBI has released a Cyber Security framework specially designed for Rural Cooperative Banks (RCBs). This initiative will help create baseline security architecture across all RCBs that can be scaled further as and when needed.



RCBs which are members/sub-members of CPS having their own ATM Switch & SWIFT interface, hosting data centre/providing s/w support to other banks

RCBs having direct members of CPS, ATM Switch & SWIFT Interface

All RCBs, which are sub members of Central Payment System

All RCBs

Requirements of Cyber Security & NASMS alignment:

Annexure I – Baseline Cyber Security and Resilience Requirements
(Applicable all RCBs)

Inventory Management of Business IT Assets	Board approved Cyber Security Policy	Preventing access of unauthorised software	Environmental Controls	Network Management & Security
Secure Configuration	Anti-virus & Patch Management	User Access Control / Management	Secure mail and messaging systems	Removable Media
User / Employee / Management Awareness	Customer Education and Awareness	Backup and Restoration	Data Leak Prevention Strategy	Vendor / Outsourcing Risk Management
Supervisory Reporting Framework – Reporting of Cyber incidents	Chief Information Security Officer (CISO)	IT Steering Committee	Information Security Committee	Audit Committee of Board (ACB)

Annexure II – Baseline Cyber Security and Resilience Requirements
(In addition to the requirements given in Annexure - I)

Network Management & Security	Secure Configuration	Application Security Life Cycle (ASLC)	Change Management
Periodic Testing	User Access Control / Management	Authentication Framework for Customers	Anti-Phishing
User / Employee / Management Awareness	Audit Logs	Incident Response & Management	

Annexure III – Baseline Cyber Security and Resilience Requirements
(In addition to the requirements given in Annexure – I & II)

Network Management & Security	Secure Configuration	Application Security Life Cycle (ASLC)	User Access Control
Advanced Read-Time Threat Defence & Management	Maintenance, Monitoring, & Analysis of Audit Logs	Incident Response & Management	Risk based transaction monitoring

Annexure IV – Baseline Cyber Security and Resilience Requirements
(In addition to the requirements given in Annexure – I, II & III)

Arrangement for continuous surveillance – Setting up of Cyber Security Operation Centre (C-SOC)	Participation in Cyber Drills	Incident Response & Management
Forensics & Metrics	IT Strategy & Policy	IT & IS Governance Framework

NASMS: Software as a Service (SaaS) solution

NASMS software focus on IT Asset life cycle management. We provide **Software as a Service (SaaS)** solutions in IT Asset Management, Network Traffic Analysis, Vulnerability Management and providing state of art SOC framework to meet your security needs and stay aligned to leading compliance and framework. We work on on-premises solution as well as leading cloud platform such as AWS, Azure, etc.

1.0 Asset Management

- Asset Inventory
- Asset Classification
- Asset Monitoring
- Asset Notification

4.0 i - SOC Management

- Asset Management
- NTA Management
- Vulnerability Management
- Incident Management
- Response management
- Forensic Analysis

2.0 Network Traffic Analysis

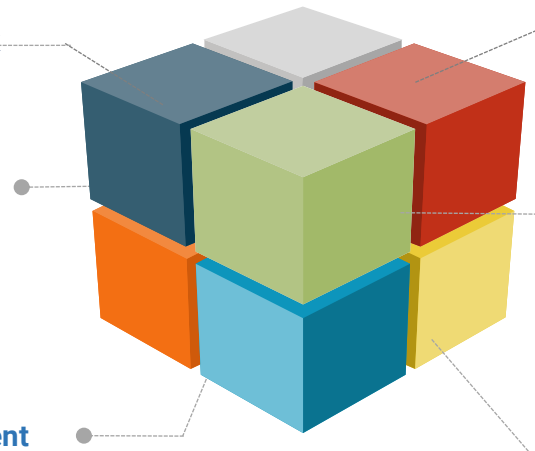
- Network monitoring
- Network Traffic Analysis
- Network Utilization
- Network Notification
- Firewall Rules

3.0 Vulnerability Management

- Vulnerability monitoring
- Vulnerability Dashboard
- Vulnerability Investigation
- Vulnerability Notification
- Up to date vulnerability database

NASMS: Consultancy as a Service (CaaS) solution

We offer **Consultancy as a Service (CaaS)** in Cyber Security compliances, implementation and training programs, awareness programs for cybersecurity frameworks & audits.



1.0 RBI Cyber Security Framework

6.0 Cyber Security Awareness & Trainings

2.0 Cyber Security Assessment & Compliance

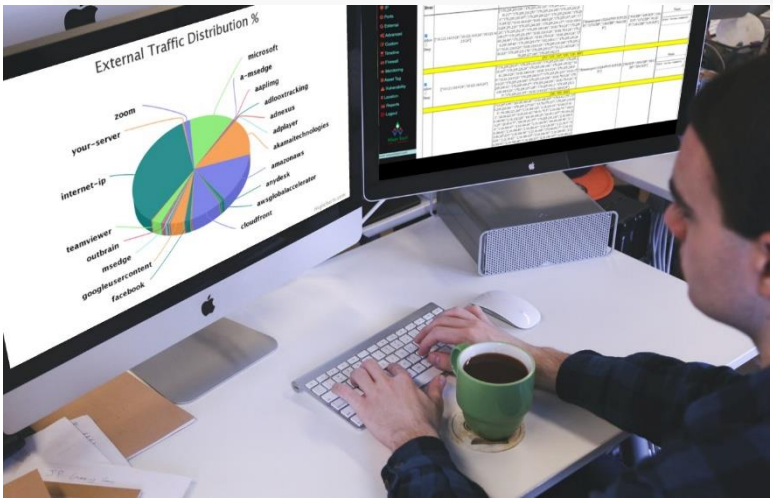
5.0 Leading compliance & Audit (BSA, GDPR, OSFI, PCI, DSS, NIST, HIPPA etc.)

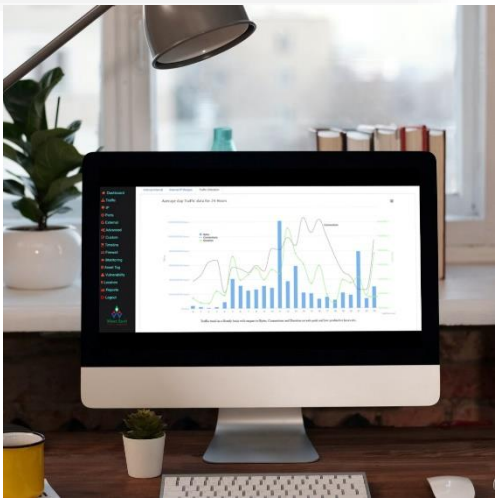
3.0 Risk management strategy

4.0 Business Continuity Frameworks compliance & DR management

NASMS interface & Customized Dashboards:

We offer 24x7 customisable dashboards which are aligned with Monitoring Configuration Templates, Alert Filtering, Anamolies Detection, Graphical views, Geographical views, Network Traffic Analysis & Vulnerabilities Management. We embed various dashboards to create SOC dashboard.





NASMS Service Modules:

	Particulars	Service Pack 1	Service Pack 2	Service Pack 3
Asset Management	Asset Discovery	√	√	√
	Critical Assets Availability Monitoring	√	√	√
	Real Time Assets Utilization	√	√	√
	Asset Notification		√	√
Network Traffic Analysis	Network Analysis	√	√	√
	Real Time Network Monitoring	√	√	√
	Network Utilization	√	√	√
	Network Notification		√	√
Vulnerability Management	Vulnerability Monitoring of Critical Assets	√	√	√
	Vulnerability Dashboard	√	√	√
	Vulnerability Investigation		√	√
	Vulnerability Notification		√	√
Advance Analysis	Anomalies detection	√	√	√
	Internal IP ranges to external traffic	√	√	√
	Vulnerable Port Traffic Analysis		√	√
	Smart Assets Tagging		√	√
	Advance level firewall rules creation			√
	Micro level Network connectivity analysis			√
	Rule Assist (Business Relevance & Non-Relevance)			√
	Root Cause Analysis			√
Customizable Service	Graphical Views	√	√	√
	Geographical Views		√	√
	Dynamic Interactive Informative Graphs		√	√
	Customizable Configuration Template			√
SOC Service	Asset Management		√	√
	Network Traffic Analysis Management		√	√
	Vulnerability Management			√
	Onsite support by SME			√
	Cyber Security awareness programs & trainings			√

For more details, please get in touch with us at: sales@wissenbaum.com

Wissen Baum
Software Solutions

USA

100 West
Big Beaver Road
Suite 200 Troy,
MI 48084 United States
Contact: +1 248 823 8114

Europe

Breslauer
Str 16,
38440 Wolfsburg
Germany
Contact: +49 159 067 435 96

India (Pune)

Office no B 113,
B wing, Ganga Osian
Square, Kaspate Vasti,
Wakad, Pune 411057
Contact: +91 82 377 00 669

India (Delhi)

446, JMD Megapolis,
Sohna Road,
Sector – 48,
Gurgaon – 122018
Contact: +91 82 377 00 660

info@wissenbaum.com

www.wissenbaum.com