LTS Secure

LTS Secure Cyber Security Framework

Actionable Guideline For Standard Banks

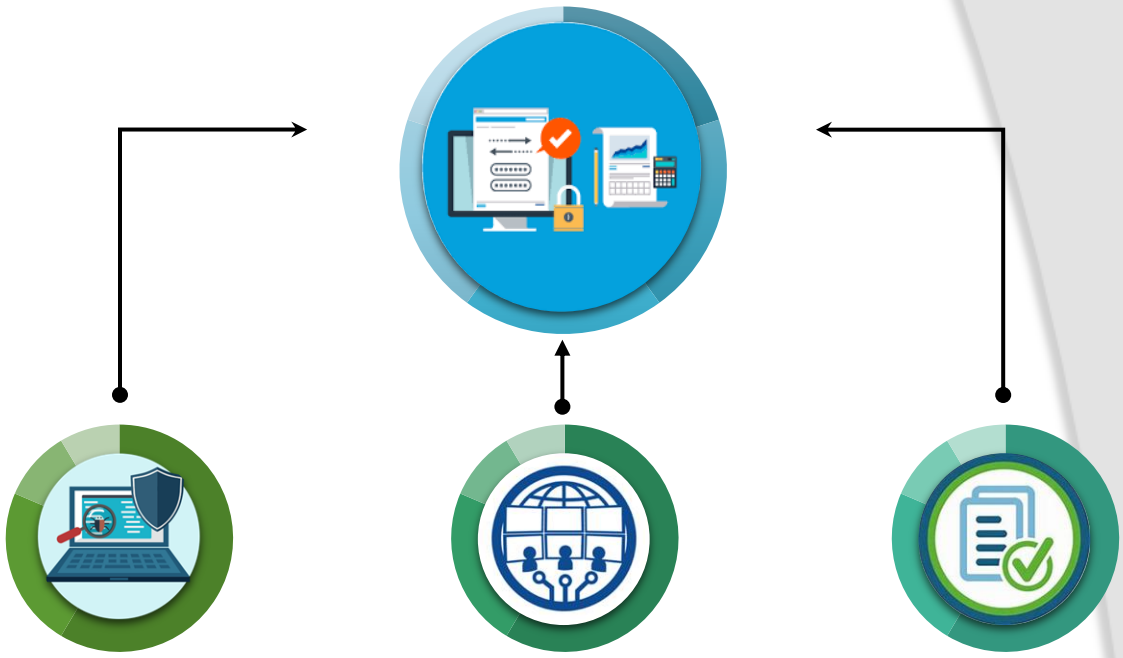
RBI Security Framework

RBI has released a guideline for cyber security framework specially designed for Banks. This guideline highlights the requirement put into focus for robust cyber security and resilience framework. This will enable Banks to formalize and adopt cyber security policy and cyber crisis management plan. Also, help to create a baseline security architecture across all banks that can be scaled further as and when needed. This framework also provides a non-exhaustive list of known cyber threats to focus upon.

Entailment of RBI Requirements proposed guidelines for Banks:

Cyber Security Policy	Elucidate and adopt a comprehensive Cyber Security Framework that includes: ☞ Cyber Security Strategy ☞ Cyber Security Policy & Procedures ☞ Assessment of cyber threats and risks
Continuous Surveillance	Create cyber security assessment test to identify vulnerabilities and security flaws in Bank's infrastructure or applications on a interval basis.
IT Architecture	Build Cyber Security Operations Centre (C-SOC) for proactive monitoring using sophisticated tools for detection, quick response and backed by tools for data analytics.
Networking And Database Security	Perform comprehensive review of network (firewall rules, opening/closure of ports, etc.) and database (direct database access, back-end updates, etc.) security. Define and document processes access to networks and databases for valid business or operational requirement.
Customer Information	Responsible for securing customer information even when it is with the customer or with third party vendor.
Cyber Crisis Managenment Plan	Develop Cyber Crisis Management Plan (CCMP) based on: ☞ National Cyber Crisis Management Plan (CERT-IN) ☞ Cyber Security Assessment Framework (CERT-IN) ☞ CERT-In/NCIIPC/RBI/IDRBT guidance Review BCP/DR program and align BCP/DR with Cyber Crisis Management Plan (CCMP).Implement preventive, detective, and corrective controls to protect Bank against cyber-threats, and to promptly detect, respond, contain, and recover from any cyber-intrusions.
Cyber Security Preparedness Indicators	Define indicators to assess and measure adequacy of and adherence to cyber security and resilience framework. Use indicators for comprehensive testing through independent compliance checks and audits carried out Cyber Security by qualified professionals.
Reporting Cyber Incident	Strengthen information security incident monitoring and management processes. to include cyber security incidents and attempts. Update incident management policy and procedures to sanitize and share cyber security related incidents on forum's such as CISO forum, and IB-CART.
Organization Structure	Review information security organization structure, CISO's roles and responsibilities to ensure that cyber security concerns are adequately highlighted within the Bank.
Cyber Security Awareness	Conduct Cyber Security Awareness and Training sessions for all relevant stakeholders of the Bank including Board of Directors, Top Management, Third Party Vendors, Customers, Employees.

LTS Secure Aid In Achieving Compliance To RBI Cyber Security Framework



Cyber Security and Resilience Requirements
Inventory Management of Business IT Assets
Preventing execution of unauthorised software
Environmental Controls
Network Management and Security
Secure Configuration
Application Security Life Cycle (ASLC)
Patch/Vulnerability & Change Management
User Access Control / Management
Authentication Framework for Customers
Secure mail and messaging systems
Vendor Risk Management
Removable Media
Advanced Real-time Threat Defence and Management
Anti-Phishing
Data Leak prevention strategy
Maintenance, Monitoring, and Analysis of Audit Logs
Audit Log settings
Vulnerability assessment and Penetration Test and Red Team Exercises
Incident Response & Management
Risk based transaction monitoring
User / Employee/ Management Awareness
Customer Education and Awareness

Cyber Security Operation Centre (C-SOC)
Security Governance
Conduct Incident Management And Forensic Analysis
Co-Ordination With Contact Groups Within The Bank/External Agencies
Implementation External Integration
Identifying A Suitable Model For Implementation
Process Related Aspects
Resolving Technology Issues

Security Incident Reporting (SIR)
Process For Reporting Cyber Incidents
Cyber Security Incident Reporting (CSIR) Form
Security Incident Reporting within two to six hours

How Can LTS Secure Help In Implementing RBI Guidelines?

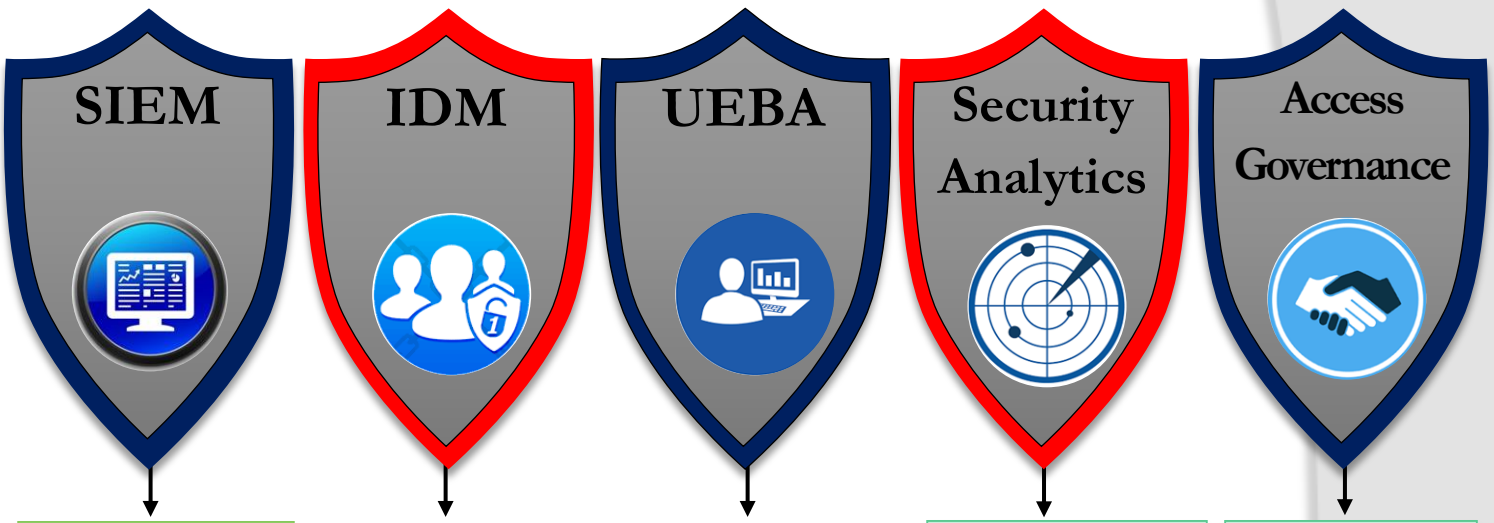
Banks acknowledge the magnitude of the problem that cyber risks pose. A deeper analysis of the successes and failures of cyber security programs shows that Banks need to develop a more comprehensive approach to cyber risk management as also suggested by RBI in their guidelines for Cyber Security Framework

LTS Secure platform was developed to deliver scalable, innovative & flexible security solution to the Banks struggling with security monitoring, access governance and identity management. LTS offers a broad array of products and features aimed at helping Banks to address both simple and complex activities. With our intelligent driven SOC, you can perform security operations, reporting analysis, and management capabilities to support operational security infrastructure.

LTS Secure Service Suite is a complete security monitoring package, which provides you cutting edge technology and trusted products. Also, aid banks to improve security posture with Industry-leading practices, insights from cyber incidents, and awareness of regulatory standards.

Our Integrated Service suite comprises of following products:

- SIEM (Security Information & Event Management)
- IDM (Identity and Access Management; Cloud Access Security Broker)
- UEBA (User Entity Behavioural Analytics)
- Security Analytics (Centralize Log Management and Network Behavioural Analytics)

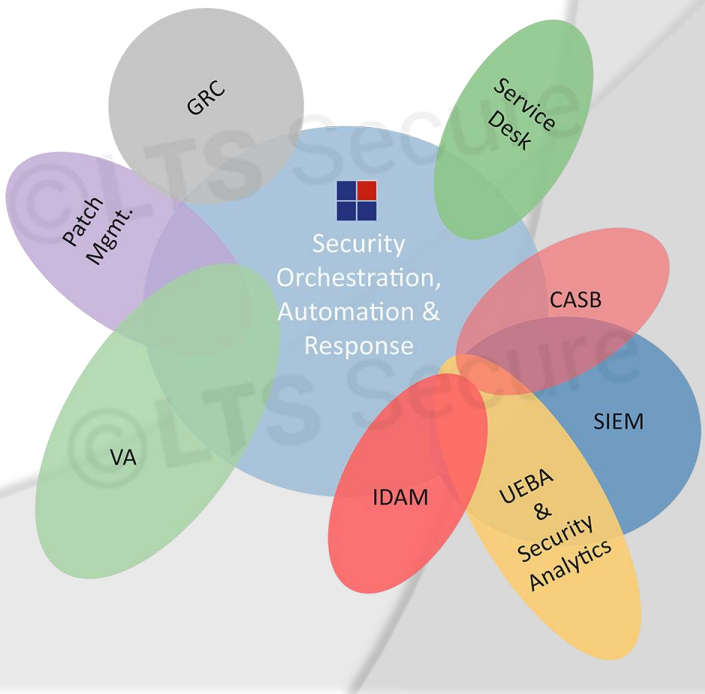


IT Architecture	Cyber Security Preparedness Indicators	Continuous Surveillance	Cyber Crisis Management Plan	Access Recertification
Reporting Cyber Incident	Organization Structure	Customer Information	Networking And Database Security	Privilege Identity Management
Cyber Security Policy			Cyber Security Awareness	

By implementing LTS SOAR stack you can improve the efficiency of your security operations through a series of aligned capabilities and processes. It begins with broad and deep visibility across your IT environment and ends with rapid mitigation and recovery from a security incident.

ABOUT LTS SECURE

LTS secure is an integrated security platform (SIEM + UEBA + CASB + IDM) that enables continuous monitoring & detection of threats, vulnerabilities and risk of it network, applications and by users in a single pane based on security orchestration, automation and response.



LTS Secure

For Enquiry: enquiry@leotechnosoft.net | info@leotechnosoft.net

+13235445013 | +15742138310 | www.ltssecure.com