CYBERSRC®
SECURITY RISK COMPLIANCE
Simplifying Cyber Risk Management..

CyberSRC® Solution Document

System Audit Report for Data Localisation (SAR)

Setting the Context

CERT-In Empanelled SAR for Data Localization & Storage of Payment System Data is a compliance mandate driven by RBI to ensure appropriate security measures and data localization controls for storage of payment related data.

What is Data Localisation?

Data localisation is the practice of storing data on any device that is physically present within the borders of the country where the data is generated. As of now, most of these data are stored, in a cloud, outside India.

Advantages of Data Localisation:

- Unfettered supervisory access to data will help Indian law enforcement ensure better monitoring.
- It will give local governments and regulators the jurisdiction to call for the data when required.
- Data centre industries are expected to benefit due to the data localization which will further create employment in India.
- Minimizes conflict of jurisdiction due to cross-border data sharing and delays in justice delivery in case of a data breach.
- Secures citizen’s data and provides data privacy and data sovereignty from foreign surveillance.
- Ensures National Security by providing ease of investigation to Indian Law Enforcement agencies as they currently need to rely on Mutual Legal Assistance Treaties (MLATs) to obtain access to data.
- Greater accountability from firms about the end-use of data.

RBI Notification

The Reserve Bank of India (RBI) issued a notification to mandate the storage of all end-to-end transaction data within India on April 8, 2018. RBI, the central banking institution, controlling monetary policies in India, requires unrestricted supervisory access to all the payment data and hence this mandate. Data Localization can be referred to as a government policy for storing the user data collected within its jurisdiction on the servers located within the country.

- Reserve Bank of India authorizes all global and local transaction operators in India to preserve all end-to-end payment data "within the country" has been whispering in the present payment environment across the world.

- The authorization is relevant for every organization handling payment data – initiating from fintech firms that perform peer-to-peer payment transactions to gateway operators which are accessed globally for universal funds transactions.

Circular for Payment Operators

- The Reserve Bank of India issued a directive vide circular DPSS.CO.OD.No 2785/06.08.005/2017-18 dated April 06, 2018, on ‘Storage of Payment System Data’ advising all system providers to ensure that, within six months, the entire data relating to payment systems operated by them is stored in a system only in India.
- This data should include the full end-to-end transaction details/information collected/ carried/processed as part of the message/payment instruction.
- System providers shall submit the System Audit Report (SAR) on completion of the requirement. The audit should be conducted by **CERT-IN Empanelled Auditors** certifying completion of an activity. The SAR duly approved by the Board of the system providers should be submitted to the Reserve Bank.

Key requirements for SAR

As per RBI and NPCI guidelines

Payments Data Elements –SAR check all data elements and their classification as payments and non-payments data. It should cover customer data, payment sensitive data, payment credentials, and transaction data. Each element needs to be categorized into jurisdictions and whether or not the data has been brought back to India.

Application Architecture – Detailed application architecture indicating where the application modules/components are located geographically.

Cross Border Transactions - The report should clearly state whether any cross-border transactions are supported by the applications.

Data Storage - The report should bring out, that defined payment data is only stored in India and no copy/backup is maintained outside the Indian jurisdiction in any form.

Transaction/Data Flow- Detailed transaction/data flow should be included with the step-wise explanation of how the transaction flows and cover application modules/components through which each of the data elements will pass through or get stored in India.

Network Diagram/Architecture - Detailed network architecture for both Primary (PR) and Disaster Recovery (DR) sites showing the relevant equipment including CBS wherever applicable.

Activities after Payment Processing - SAR should identify activities after payment processing like settlement processing and check if these processes are carried out in India or outside India.

Access Management – SAR should define whom all have access to the payments data and what kind of access has been granted to respective individuals/ teams.

Key requirements for SAR

As per RBI and NPCI guidelines

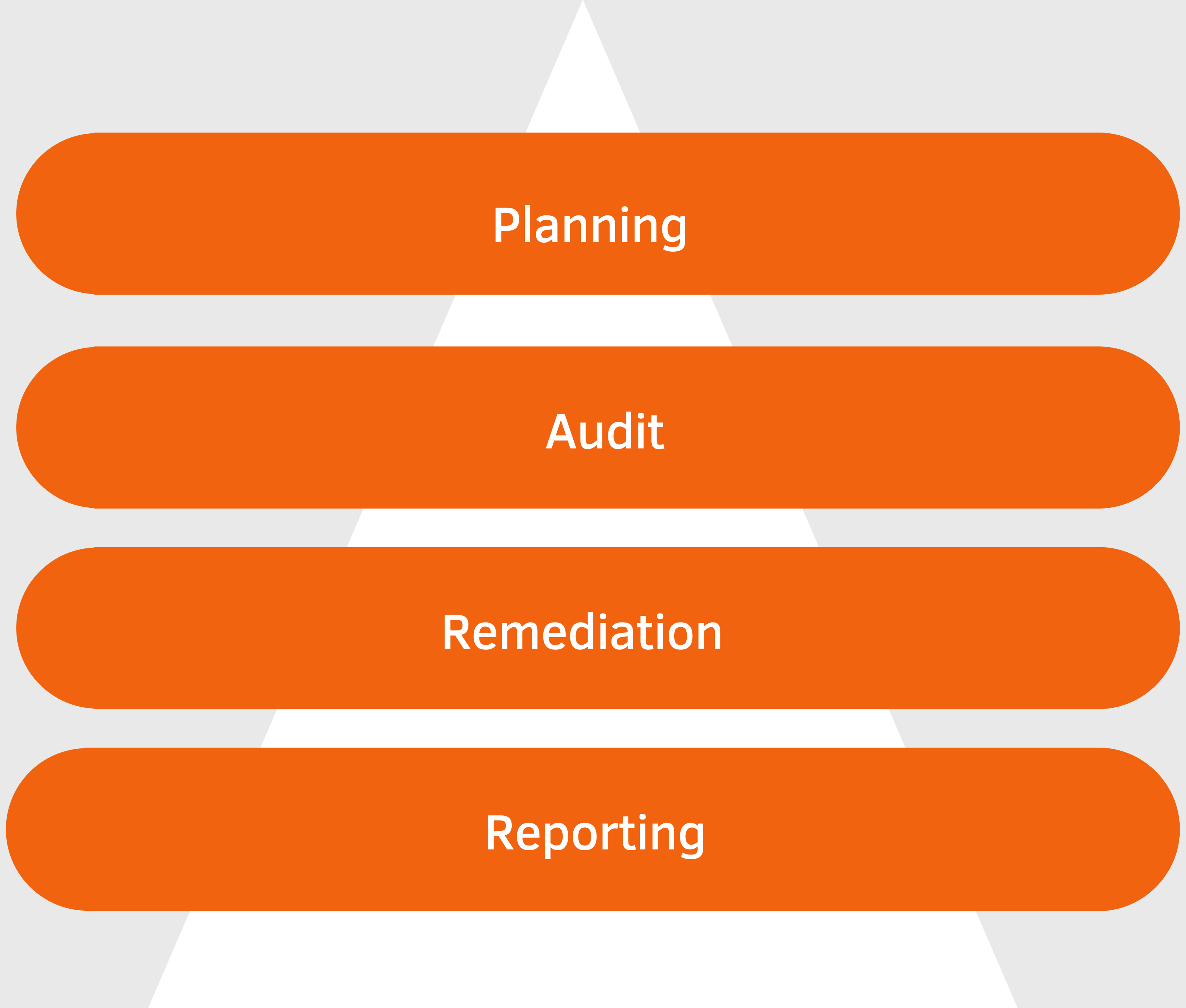
Data Security – The SAR from a CERT-In empanelled Auditor, must be verified to ensure transaction data is safeguarded. This includes data storage, maintenance of database, data backup restoration, data security, etc.

Transaction Processing - It should check if aspects of transaction processing are done in India and outside India. In the case of outside India, purging policy/process for the processed payments data shall be mentioned in the report.

Reporting-

- SAR should adequately address RBI Data Localization FAQs and other compliances that could be released from time to time.
- For new apps going live from FY 2020-21, it is advised to share the Data Localization SAR in line with the above expectations.
- In addition to this, whenever there is any change in the architecture of the application thereby changing the jurisdiction of the payment data elements stored, participants shall inform NPCI.
- Also whenever there is a change of primary or disaster recovery site, participants should inform NPCI of the change.

CyberSRC' approach for System Audit Report for Data Localization is covered in 4-phases:



Planning

Audit

Remediation

Reporting

Phase 1: Information Gathering and Planning

Initially, various documentation and evidences are collected on the architecture, implementation and controls to understand data flow then start planning and preparation of the audit scope and objectives accordingly.

Phase 2: Audit

We conduct an initial audit for understanding the organization's infra and help the organization in identifying all the storage locations which comprise any payment-related data.

Phase 3: Audit Performance Remediation

If any payment data is identified, we will provide remediation support for complying with the RBI mandate.

Phase 4: Reporting

In the final phase, we review report audit findings, conclusions, and recommendations of the audit in terms of conformance, non-conformance, and opportunities to improve and share the confirmation letter that, all payment-related data is residing inside India.

How can CyberSRC® help?

CyberSRC® is a CERT-in Empanelled Security Audit organization that has the expertise and experience to help your organization with the compliance process and fulfill SOC reporting requirements and the Trust Service Principles. Our team of professionals will secure your data in a cost-efficient manner to give you and your client base the peace of mind you deserve. Our work will help in increased client trust, brand reputation boost, and more robust data privacy and confidentiality.

As a CERT-In Empanelled Auditor, we document the entire activity along with relevant documentation, artifacts, findings, recommendations, etc.

'CyberSRC® is an ISO 27001 Certified and CERT-In Empanelled Security Auditing Organization'

CyberSRC®
Through the Years

● Our history at a glance

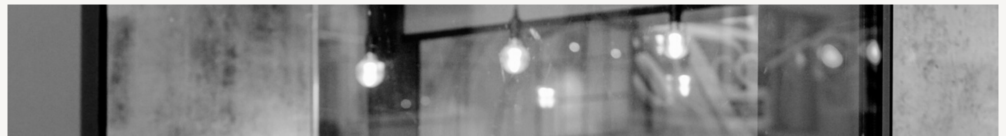
Established in January 2018, CyberSRC® is a CERT-in Empanelled Security Audit Organization that offers the full gambit of cybersecurity services ranging from threat intelligence to general advisory services in areas pertaining to Cybersecurity such as Vulnerability attacks, compliance, and cybersecurity regulations, and laws.

CyberSRC® within a short span of three years has mitigated cyber risks across a broad spectrum of clients. For instance, there are organizations that require system auditing. This involves complying with various regulations and laws.

Our Team

We are a team of qualified professionals with rich experience in multiple industries such as Manufacturing, BFSI, Insurance, Healthcare, NBFCs & others.
Our consultants and auditors are industry experts and have proven track records, some of the renowned certificates that our consultants hold such as CISA, CIPM, CISSP, COBIT, CEH, CCNA, OSCP, ISO 9001 LA/LI, ISO 27001, ITIL LA/LI, PMP, to name a few. We believe in adding value to your business which is enabled through our Centre of Excellence (Coe) and, we have the end-to-end capability for Program Build–Operations Transformation.

Backed by a very diverse and dynamic team which have a combined experience of 35 years under the belt



Our Services

INFORMATION SYSTEM ASSURANCE & AUDIT

VULNERABILITY AND PENETRATION TESTING SERVICES

EXTERNAL THREAT INTELLIGENCE

RISK COMPLIANCE ADVISORY

PHISHING CAMPAIGNS/ STIMULATION

REGULATORY COMPLIANCE AUDIT (RBI, IRDA, SEBI)

PRIVACY AND DATA PROTECTION COMPLIANCE AND AUDIT

INCIDENT RESPONSE & MALWARE ANALYSIS

ISO IMPLEMENTATION & ADVISORY (ISO 27001, 9001, 27701)

Network & Cloud Security

Our Esteem Clients

भारतीय वायु सेना
INDIAN AIR FORCE
GOVERNMENT OF INDIA
Spice money
EPOCH
WE SERVE ONTIME EVERYTIME
Monkeycap
Be sure when you insure
knowlarity
AnyTimeLoan.in™ BETA
Need it. Get it.
ICICI Securities
wipro
techmatrix
CONSULTING
Denave
Sales.Enabled
EPIC Private Equity
UZIO
UNO MINDA
NK MINDA GROUP
EBIX
SANNAM S4
EXPLORE • ENTER • EXPAND
EUGENIX
HAIR SCIENCES
compport
Afflatus
SMART DOCUMENT SOLUTIONS
7Con
Balaji Mariline
RISKBERG
STONEWAIN
SYSTEMS INC
Virtual Clone
Think Talent™
SERVICES

Disclaimer: Some of the above clients are not our direct clients but we have provided services as part of larger engagement

Contact Us

WEBSITE

www.cybersrcc.com

EMAIL

info@cybersrcc.com pre-sales@cybersrcc.com

CONTACT NUMBER

+91 8800377255

HEAD OFFICE

Unit 605, 6th floor, World Trade
Tower, Sector 16, Noida (UP)
-201301, India

OTHER OFFICE

London (UK): Kemp House
152 160 City Road,
London , UK (EC1V 2NX)