भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/2013-14/335
RPCD.CO.RRB.BC.No.45 /03.05.33 /2013-14 October 24, 2013

The Chairmen
All Regional Rural Banks

Dear Sir,

Sharing of Information Technology Resources by Banks - Guidelines

Please refer to paragraph 101 of the Monetary Policy Statement 2013-14 wherein the need for banks to examine the issue of shared IT resources to optimise costs while maintaining the desired levels of efficiency and security has been emphasised.

2. One of the pre-requisites for a bank to consume shared IT resources is the existence of a strong IT and IS Governance in the bank. It is imperative that decisions on IT resource sharing have necessary approvals of the management possibly at the board level depending on the criticality of the infrastructure or application to be shared. The applications that can be considered for sharing IT resources are those related to collaboration, housekeeping, office automation and business applications.

3. As a consumer, Regional Rural Banks may ensure that the service provider (including another bank) adheres to all regulatory and legal requirements of the country. Regional Rural Banks may necessarily enter into agreement with the service provider that the infrastructure and applications are made available for audit / inspection by the regulators of the country. Reserve Bank of India and NABARD should have access to all information resources that are consumed by Regional Rural Banks, though the resources are not physically located in the premises of banks. Further, Regional Rural Banks have to adhere to the relevant legal and regulatory requirements relating to geographical location of infrastructure and movement of data out of borders.

4. While consuming services provided by other banks or service providers, it may be ensured that all aspects relating to privacy, confidentiality, security and business continuity are fully met.

5. A document which may serve as guidance in this regard is enclosed.

6. Please acknowledge receipt of the letter to our concerned Regional Office.

Yours faithfully,

(A.Udgata)
Principal Chief General Manager

चेतावनी: रिज़र्व बैंक द्वारा ई-मेल, डाक, एसएमएस या फोन कॉल के जरिए किसी की भी व्यक्तिगत जानकारी जैसे बैंक के खाते का ब्यौरा, पासवर्ड आदि नहीं मांगी जाती है। यह धन रखने या देने का प्रस्ताव भी नहीं करता है। ऐसे प्रस्तावों का किसी भी तरीके से जवाब मत दीजिए।

Caution: RBI never sends mails, SMSs or makes calls asking for personal information like bank account details, passwords , etc. It never keeps or offers funds to anyone. Please do not respond in any manner to such offers.

Sharing of Information Technology Resources by Banks - Steps

1. Identify the asset(s) to be included:

   a. Data
   b. Applications/Functions/Process

2. Evaluate the asset on the following factors-

   a. Determine how important the data or function is to the bank
   b. Analyse the impact of the scenarios
      i. The asset becoming widely public & widely distributed
      ii. An employee of the service provider accessing the asset
      iii. The process or function being manipulated by an outsider
      iv. The process or function failing to provide expected results
      v. The info/data being unexpectedly changed
      vi. The asset being unavailable for a period of time

3. Choose the external organisation carefully:

   a. A bank
   b. An IT Company
   c. Any other organization

4. Map Data Flow

   a. Map the data flow between bank, service provider, customers, other nodes
   b. Essential to understand whether data can move in/out of the shared infrastructure provided by others
   c. Sketch it for each of the models
   d. Know risk tolerance

5. Assess requirements

   a. Infrastructure
   b. Applications

6. Analyse the Security Concerns

   a. Issues in applications - Service levels, security, governance, compliance, liability expectations of the service provider are contractually defined
   b. Issues in infrastructure - service provider handling Infrastructure security

7. Prepare a service contract addressing the following domains:

   a. Architectural Framework
   b. Governance, Enterprise Risk Management
   c. Legal, e-Discovery
   d. Compliance & Audit
   e. Information Lifecycle Management
   f. Portability & Interoperability
   g. Security, Business Continuity, Disaster Recovery
   h. Data Center Operations
   i. Incident Response Issues
   j. Application Security
   k. Encryption & Key Management
   l. Identity & Access Management
   m. Virtualization

8. Understand the issues in security pitfalls

   a. Geographical location of Infrastructure
   b. Scope network security issues
   c. Control Mechanism

9. Comprehend the overall security concerns

   a. Handing over operational control to service provider while maintaining accountability

10. General Governance issues

    a. Identify, implement process, controls to maintain effective governance, risk management, compliance
    b. Provider security governance should be assessed for sufficiency, maturity, consistency with user ITSEC process

11. 3rd Party Governance issues

    a. Request for clear documentation on how facility & services are assessed
    b. Requirement of definition of what provider considers critical services, information
    c. Perform full contract, terms of use due diligence to determine roles, accountability

12. Analyse legal issues

    a. Functional: functions & services which have legal implications for both parties
    b. Jurisdictional: which governments administer laws and regulations impacting services, stakeholders, data assets
    c. Contractual: terms & conditions

d. Clarity on provider and consumer's roles
e. Litigation hold
f. e-Discovery searches
g. Expert testimony
h. Provider must save primary and secondary (logs) data
i. Location of storage data
j. Plan for unexpected contract termination and orderly return or secure disposal of assets
k. Ensuring retention of ownership of data in its original form

13. Examine compliance & audit function

a. Right to Audit clause
b. Analyze compliance scope
c. Regulatory impact on data security
d. Evidence requirements are met
e. Appropriate certification such as SAS 70 Type II, ISO 27001/2 audit statements

14. Study Information Lifecycle Management especially in the context of

a. Data security
b. Data Location
c. All copies, backups stored only at location allowed by contract, SLA and/or regulation

15. Analyse portability and interoperability

a. Factors necessitating switching service providers
b. Negotiate Contract price increase
c. Factor in service provider bankruptcy and service shutdown
d. Decrease in service quality
e. Business dispute

16. Understand security, business continuity, disaster recovery related issues

a. Centralization of data means greater insider threat from within the provider
b. Requirement of onsite inspections of provider facilities
c. Disaster recovery, Business continuity, of service provider etc.

17. Formulate appropriate Incident Response systems

a. Applications may not always be designed with data integrity, security in mind
b. Necessity to store keep application, firewall, IDS etc. logs
c. Management of snapshots of virtual environment

18. Plan application security

    a. Different trust boundaries for various types of shared resources
    b. Ensure web application security
    c. Secure inter-host communication channel

19. Devise encryption, key management procedures

    a. Encrypt data in transit, at rest, backup media
    b. Secure key store
    c. Protect encryption keys
    d. Ensure encryption is based on industry/government standards
    e. Limit access to key stores
    f. Key backup & recoverability
    g. Test these procedures

20. Manage ID, access control

    a. Determine how service provider handles provisioning, de-provisioning
    b. Authentication
    c. Federation
    d. Authorization
    e. User profile management

21. Plan virtualization

    a. Type of virtualization
    b. 3rd party security technology augmenting virtual OS controls that protect admin interfaces

----