ANNEXURE–A

IS Audit Scope

Indicative scope of IS Audit is given below:

The indicative scope of IS Audit is given below:

- Alignment of IT strategy with Business strategy
- IT Governance related processes
- Long term IT strategy and Short term IT plans
- Information security governance, effectiveness of implementation of security policies and processes
- IT Architecture
  - Acquisation and Implementation of Packaged software
    - Requirement Identification and Analysis
    - Product and Vendor selection criteria
    - Vendor selection process
    - Contracts
    - Implementation
    - Post Implementation Issues
  - Development of software- In-house and Out-sourced
    - Audit framework for software developed in house, if any
    - Software Audit process
      - Audit at Program level
      - Audit at Application level
      - Audit at Organizational level
    - Audit framework for software outsourcing
  - Operating Systems Controls
    - Adherence to licensing requirements
    - Version maintenance and application of patches
    - Network Security
    - User Account Management
    - Logical Access Controls
    - System Administration
    - Maintenance of sensitive user accounts
  - Application Systems and Controls
    - Logical Access Controls
    - Input Controls
    - Processing Controls
    - Output Controls
    - Interface Controls
    - Authorization Controls
    - Data Integrity/ File Continuity controls
    - Review of logs and audit trails
  - Database Controls
    - Physical access and protection
    - Referential Integrity and accuracy
    - Administration and Housekeeping

  - Network Management audit
    - Process
    - Risk acceptance (deviation)
    - Authentication
    - Passwords
    - Personal Identification Numbers ('PINS')
    - Dynamic password
    - Public key Infrastructure ('PKI')
    - Biometrics authentication
    - Access Control
    - Cyptography
    - Network Information Security
    - E-mail and Voicemail rules and requirements
    - Information security administration
    - Microcomputer/ PC security
    - Audit trails
    - Violation logging management
    - Information storage and retrieval
    - Penetration testing
- Physical and environmental security
- Maintenance
  - Change Request Management
    - Software developed in-house
  - Version Control
  - Software procured from outside vendors
  - Software trouble-shooting
    - Helpdesk
  - File/ Data reorganization
  - Backup and recovery
    - Software
    - Data
    - Purging of data
  - Hardware maintenance
  - Training
- Internet Banking
  - Information systems security framework
  - Web server
  - Logs of activity
  - De-militarized zone and firewall
  - Security reviews of all servers used for Internet Banking
  - Database and Systems Administration
  - Operational activities
  - Application Control reviews for internet banking application
  - Application security
- Privacy and Data Protection
  - Controls established for data coversion process
  - Information classification based on criticality and sensitivity to business operations

- Fraud prevention and Security standards
- Isolation and confidentiality in maintaining of Bank's customer information, documents, records by banks
- Procedures for identification of owners
- Procedures of erasing, shredding of documents and media containing sensitive information after the period of usage.
- Media control within the premises

- Business Continuity Management
  - Top Management guidance and support on BCP
  - The BCP methodology covering the following:
    - Identification of critical business
    - Owned and shared resources with supporting function
    - Risk assessment on the basis of Business Impact Analysis ('BIA')
    - Formulation of Recovery Time Objective ('RTO') and Identification of Recovery Point Objective('RPO')
    - Minimising immediate damage and losses
    - Restoring of critical business functions, including customer-facing systems and payment settlement systems
    - Establishing management succession and emergency powers
  - Addressing of HR issues and training aspects
  - Providing for the safety and wellbeing of people at branch or location at the time of disaster
  - Assurance from Service providers of critical operations for having BCP in place with testing performed on periodic basis.
  - Independent Audit and review of the BCP and test result
  - Participation in drills conducted by RBI for Banks using RTGS/ NDS/ CFMS services
  - Maintaining of robust framework for documenting, maintaining and testing business continuity and recovery plans by Banks and service providers
- Asset Management
  - Records of assets mapped to owners
  - For PCI covered data, the following should be implemented:
    - Proper usage policies for use of critical employee facing technologies
    - Maintenance of Inventory logs for media
  - Restriction of access to assets through acceptable useage policies, explicit management approval, authentication use of technology, access control list covering list of employees and devices, labeling of devices, list of approved company products, automatic session disconnection of remote devices after prolong inactivity
  - Review of duties of employees having access to asset on regular basis.
- Human Resources
  - Recruitment policy and procedures for staff
  - Formal organization chart and defined job description prepared and reviewed regularly
  - Proper segregation of duties maintained and reviewed regularly
  - Prevention of unauthorized access of Former employees
  - Close supervision of staff in sensitive position
  - People on notice period moved in non-sensitive role
  - Dismissed staff to be removed from premises on immediate effect

- IT Financial Control
  - Comprehensive outsourcing policy
  - Coverage of confidentiality clause and clear assignment of liability for loss resulting from information security laspe in the vendor contract
  - Periodic review of financial and operational condition of service provider with emphasis to performance standards, confidentiality and security, business continuity preparedness
  - Contract clauses for vendor to allow RBI or personnel authorized by RBI access relevant information/ records within reasonable frame of time.
- IT Operations
  - Application Security covering access control
  - Business Relationship Management
    - Customer Education and awareness for adoptation of security measures
    - Mechanism for informing banks for deceptive domains, suspecious emails
    - Trademarking and monitoring of domain names to help prevent entity for registering in deceptively similar names
    - Use of SSL and updated certification in website
    - Informing client of various attacks like phishing
  - Capacity Management
  - Service Continuity and availability management
    - Consistency in handling and storing of information in accordance to its classification
    - Securing of confidential data with proper storage
    - Media disposal
    - Infrastructure for backup and recovery
    - Regular backups for essential business information and software
    - Continuation of voice mail and telephone services as part of business contingency and disaster recovery plans
    - Adequate insurance maintained to cover the cost of replacement of IT resources in event of disaster
    - Avoidance of single point failure through contingency planning
  - Service Level Management
- Project Management
  - Information System Acquisition, Development and Maintenance
    - Sponsorship of senior management for development projects
    - New system or changes to current systems should be adequately specified, programmed, tested, documented prior to transfer in the live environment
    - Scrambling of sensitive data prior to use for testing purpose
  - Release Management
    - Access to computer environment and data based on job roles and responsibilities
    - Proper segregation of duties to be maintained while granting access in the following enviornment
      - Live
      - Test
      - Development
    - Segregration of development, test and operating environments for software
- Record Management

  - Record processes and controls
    - Policies for media handling, disposal and transit
    - Periodic review of Authorization levels and distribution lists
    - Procedures of handling, storage and disposal of information and media
    - Storage of media backups
    - Protection of records from loss, destruction and falsification in accordance to statutory, regulatory, contractual and business requirement
- Technology Licensing
  - Periodic review of software licenses
  - Legal and regulatory requirement of Importing or exporting of software
- IT outsourcing related controls
- Detailed audit delivery channels and related processes like ATM, internet banking, mobile banking, phone banking, card based processes
- Data centre operations and processes
  Review relating to requirements of card networks (for example, PIN security review)

ANNEXURE - B

Training Needs to Manage IT Infrastructure

In the past few years, the Indian banking sector has implemented major technology initiatives to deliver state-of-the-art and innovative banking services to the country. One of the significant projects implemented is the centralised database and centralised application environment for core and allied applications and services which is popularly known as the Core Banking Solution (CBS). Design and implementation of the CBS is complete in most of the Banks and the rest is expected to complete the same shortly.

Major components of the CBS solution include

- Data Centre and Disaster Recovery Centre
- Network Solution architecture to provide total connectivity
- Enterprise Security architecture
- Branch and Delivery channel environment

The ongoing exercise is to create a robust technology platform, which will enable a quick and easy deployment of innovative customer-oriented services in the Indian context. It is to be noted that the technology platform is expected to handle the anticipated growth in business and provide non-stop round-the-clock technology-oriented services in order to ensure:

- Performance and Scalability
- Availability and Fault Tolerance
- Security and Access control
- Conformance to standards and Interoperability

Over the past few years, Indians have been able to design and implement complex technology solution framework to ensure quantifiable and measurable metrics for the above and this has resulted in setting and meeting the expectations of the customers and stake holders.

Banking industry is no longer concentrating on the traditional approach to banking. The business model of today is entirely different compared to the last decade. Banks will continue to reinvent themselves in order to be competitive and viable. Innovative business initiatives require the technology solution to be upgraded constantly and continuously on a regular basis. Designing and implementing the solution is one aspect and more important is to effectively and efficiently manage the deployed solution to ensure that service delivery meets the expectations of business. The next section will address the important aspect of effective and efficient administration and management of the Enterprise technology solution.

Technology Management:

This section briefly covers the technology systems deployed by the Banks as a part of the CBS Project. Data Centre (DC) and the Disaster Recovery Centre (DRC) consist of the following:

- Database Environment

- Application Environment
- Web Environment
- High Performance LAN Solution
- Security solution
- Connectivity to the Corporate Network and the Internet

While the corporate network consists of:

- Core network at the DC and DRC
- Connectivity between DC and DRC for replication and other requirements
- Backbone network connecting network aggregation points to DC and DRC - Access network Connecting branches and delivery channels to NAPs - Network / Link Security using Encryption

Branch or Delivery Channels consists of:

- Access Points / Touch Points
- Local network proving connectivity
- Peripheral and Network devices

As stated earlier, in order to provide round-the-clock, non-stop services, it is mandatory that the complex technology solution deployed is managed efficiently. The success of this will depend on not only the products but more importantly the processes and people.

It is necessary to have technically competent and capable in house staff to manage the resources located at the DC and DRC, the corporate network and the branch locations. Most of the banks have outsourced the management and administration of the IT Infrastructure to the service providers and do not have the in-house capability and man power to take up the task.

Once the complete business is captured by technology and processes are automated, the Data Centre (DC) is the bank, and customers, management and staff are dependent on the DC. From a risk assessment and coverage point of view, it is important to ensure that the Bank is able to impart advanced training to its permanent staff in the core areas of technology for effective and efficient technology management and in the event of outsourcing to take over the functions at short notice at times of exigencies. Some of the broad areas that are required to be addressed are given in the next section.

Training required for Managing IT Infrastructure:

From the above two sections, it is clear that the administration and management of IT Infrastructure in the post CBS scenario is one of the major concerns of the Banking Industry and this requirement needs to be comprehensively addressed. In order to accomplish this objective it is important to have a technology institute with focus on banking and also having adequate domain knowledge for carrying out the tasks, for example, IDRBT.

The subjects and topics, which are the immediate need of the banking industry include:

vii) System Administration and Management

viii) Network Administration and Management

ix) Database Administration and Management

x) Security Administration and Management

The above listing covers the broad areas and will form the core of the training programme. About 60 to 70 percent of the training coverage will be generic in nature. The remaining will be specific to the bank, depending on the architecture and products deployed. For example, the implementation of the database layer for one CBS application is different from the other.

The next step could be to come out with details of:

- Pre-requisites required for each course
- Course coverage and Structure
- Laboratory Environment required
- Case studies to supplement the lectures

After successfully completing the course, each participant will have to undergo on-the-job training for six months to have an understanding of the systems deployed in the bank. Specific details required to manage the same on a daily basis would be understood during the period. In order to achieve optimal utilisation of the resources deployed, a clear and correct understanding of the capabilities and limitations of the systems deployed is mandatory. One of the requirements is to also look at performance tuning of the solution deployed from time to time as the requirements will vary depending on the business needs.