Checklists for Computer Audit

Index

Chapter I

INTRODUCTION

1.1 The Jilani Working Group on internal controls and inspection / audit systems in banks (1995) identified key risks associated with IT systems and recommended various control measures to address these risks. It recognized the need for a specialized system of EDP audit and recommended that the entire domain of EDP activities should be brought under the scrutiny of the Inspection and Audit department. Banks were advised by the Department of Banking Supervision (DBS) of the Bank to expeditiously implement the recommendations of the group.

1.2 The risks and controls systems in computerized banks were analysed by Coopers and Lybrand (U.K) under the Technical Assistance Project funded by the Department For International Development (DFID) U.K. Based on the consultancy report, DBS had issued in 1998 a detailed guidance note to banks apprising them of the risks in computerized environment and suggested associated controls to address the specific risk. An inspection manual was also prepared in 1997 with the assistance of the aforesaid international consultants for the guidance of the Reserve Bank officers inspecting banks with computerized accounting system. An assessment of the system of EDP audit in the concerned bank is now an integral part of the Annual Financial Inspection of banks.

1.3 An assessment of the system of computer audit in banks as on March 31, 2000 was made based on the basis of findings contained in the inspection reports of banks for the year 1998-99 and 1999-2000 and other specific feedback received from banks. Structured questionnaires were sent to all the banks eliciting information on the nature of the Information Technology (IT) management function, IT risk management and EDP audit systems, EDP audit methodology etc. The analysis revealed that the system of computer audit in banks is still in the developmental stage. A range of policy approaches has been reported in regard to the conduct of EDP audit by banks. It was observed that in respect of 50 percent of banks, the policy on IT risk management and EDP audit were not duly documented. In respect of many banks even availability of EDP inspection manuals was not ensured. The periodicity for conducting such audits also was not uniform across banks. The practice in most of the banks in India was to audit around the computer. Computer security issues did not receive adequate Top Management attention. It was evident from the assessment that the computer audit in India had been still evolving and a major constraint encountered by banks is the general shortage of skilled technical personnel for the task. The findings of the assessment were put up to the Audit Sub-committee of the Board for Financial Supervision as per the Board's direction.

1.4 The Audit Sub-committee decided that a small committee comprising representatives of RBI, ICAI, SBI, a foreign bank and a new private sector bank may be constituted to draw upon a check list in a standardised form so that all the banks operating in the country can ensure that their computerized branches are applying requisite controls in the computerized environment and the branch auditors also verify the same and report accordingly. Accordingly, a committee was constituted with Shri A.L.Narasimhan, Chief General Manager-in-Charge, Department of Banking Supervision, Central Office as the Convener.

The composition of this Committee is as follows:

1	Shri A.L.Narasimhan, Convener, Chief General Manager-in-Charge, Department of Banking Supervision, CO, Mumbai 400 005	Convener
2	Shri Ashok Kumar Chandak/ Shri R.Bupathy[1], Vice President, The Institute of Chartered Accountants of India, Indraprastha Marg, New Delhi 110 002.	Member
3	Shri S.Santhanakrishnan, Chairman, Committee on Information Technology, The Institute of Chartered Accountants of India, Indraprastha Marg, New Delhi 110 002.	Member

[1] Shri Ashok Chandak was the Vice-President of ICAI when the Committee was formed. Shri R.Bupathy substituted him as the member in the Committee consequent on his election as the new Vice-President.

4 Shri S.N.Pattnaik, Member
General Manager,
State Bank of India,
Inspection Department, Corporate Centre,
Hyderabad.

5 Shri Atilla Karasappan. Member
Vice President, Senior Country Operations Officer,
Citi Bank,
5th Floor, Plot C-61, B-K complex,
G-Block, Bandra (E),
Mumbai 400 051.

6 Shri Ashok Kumar Patni, Member
Executive Vice President & Head - Audit,
Methods & Inspection Department,
ICICI Bank Ltd,
ICICI Towers,
Bandra Kurla Complex, Mumbai 400 051.

7 Shri R.Ravikumar, Member-Secretary
Assistant General Manager,
Reserve Bank of India,
Department of Banking Supervision,
Central Office,
Mumbai 400 005.

The terms of reference of this Committee was-

To draw upon a check list in a standardised form to conduct computer audit so that all the banks operating in the country can ensure that their computerized branches are applying requisite controls in the computerized environment and the branch auditors also verify the same and report accordingly.

1.5 The Committee had its first meeting on 1st November 2001. The levels of computerization of banking industry, earlier work done in this regard and guidelines already issued by DBOD/DBS in this connection were discussed in detail. Different levels of computerization of different banks, availability of different platforms in different banks etc. were discussed and it was decided to prepare a standardised checklist for conducting computer audit. It was felt by the committee that IS Audit Checklist prepared need to be platform independent and necessary platform dependent control questionnaire can be framed by the banks themselves. Computer Audit questionnaire also should be bank independent. On the basis of the practices followed by individual banks they may frame bank specific control questionnaire.

1.6 The committee decided to classify the areas of risk in the IS environment as under:

1. Business Strategy
2. Long Term IT Strategy
3. Short Range IT Plans
4. IS Security Policy
5. Implementation of Security Policy
6. IS Audit Guidelines
7. Acquisition and Implementation of Packaged Software
8. Development of software - in-house and outsourced
9. Physical Access Controls
10.Operating System Controls
11.Application Systems Controls
12.Database controls
13.Network Management
14.Maintenance
15.Internet Banking

1.7 These areas were allotted to members of the committee to prepare relevant checklist for the respective risk areas. The checklist thus prepared was discussed by the committee in its subsequent sittings. On the basis of the deliberations a draft report was prepared and circulated to all the members for their comments. On receiving comments from the members, the checklists have been finalized and presented in the report.

Scheme of the Report

1.8 This chapter records the background for the constituting the Committee; the terms of reference and summary of recommendations of the Committee. In the next chapter, levels of computerization of banking industry, earlier work done in this regard and guidelines already issued by DBOD/DBS in this connection, different levels of computerization in banks etc. are discussed along with possible benefits of the checklists. The checklists in respect of the 15 areas of audit interest indicated in the above paragraph have been included as separate chapters in the report.

1.9 Acknowledgements

The committee places on record its gratitude to the Audi Sub-committee for constituting the committee on computer audit. The convener acknowledges the co-operation extended by all the members of the committee in completing the task entrusted and making the discussions meaningful. The keen interest shown by all the members of the committee in preparing the checklists for computer audit is appreciable. The committee acknowledges with thanks the RBI, ICAI and commercial banks for nominating senior officials for the committee and making their valuable time available. The committee further acknowledges the significant contributions made by officials of RBI, ICAI and commercial banks, who were not members but contributed in building up the checklists. Notable contributions were made by Shri R. Suriyanarayanan, ICAI, Shri Vikram Subrahmanyam and Shri Ramesh Lakshminarayanan from Citi Bank, Shri Gokul Chander from ICICI Bank, and Shri P.Parthasarathi, DGM from RBI. The committee received significant contributions from Shri.R.Ravikumar as the Member Secretary. Committee

acknowledges his dedication with gratitude and likes to record its appreciation for his outstanding work. The committee acknowledges the services of Shri M.K. Prabhu, Assistant Manager and Shri P.B.Uday in making arrangements for the meetings.

1.10 Summary of recommendations

The basic purpose for preparing checklists for conducting computer audit is to sensitize banks on the emerging concerns arising on account of computerization and growing dependency on computers and technology for conducting the business. It is expected that these checklists would bring about a minimum standard in conducting the computer audit. The checklists may be used by all the commercial banks as general guidelines for conducting computer audit. These may be circulated to appropriate levels of management so that the computer audit practices followed by banks are at least of a minimum standard. However, those banks which are following much more exhaustive checklists for conducting IS Audit / Computer Audit may continue to do so.

Recommendations:

- The checklists for conducting computer audit in commercial banks and financial institutions may be circulated to all commercial banks and financial institutions under the supervisory jurisdiction of RBI
- Banks and FIs may be advised to follow the checklists as general guidelines and those banks / institutions which are following better practices may continue to do so
- The checklists may be circulated to all the Regional Offices of DBS so as to enable the inspecting officers to conduct the computer audit at the time of financial audit. Suitable extension of time may be given to the inspecting officials
- A copy may be forwarded to Inspection Department of the Bank, who are responsible for conducting internal audit of RBI for their use
- Periodical training / seminar on this area may be conducted at RBSC (for inspecting officials of RBI) and BTC (for commercial banks) on a continuous basis
- A cell may be formed at Central Office of DBS, which will scrutinize the reports prepared by the inspecting officials so that necessary corrective action may be suggested to banks through BMDs or CPOSs as the case may be. Further this cell may continue to update the checklists with latest developments and concerns so that the checklists remain current and relevant.

A.L.Narasimhan
(Convener)
RBI

R.Bupathy	S.Santhana Krishanan	S.N. Patnaik
(Member)	(Member)	(Member)
ICAI	ICAI	SBI

Atilla Karasappan
(Member)
Citi Bank

Ashok Kumar Patni
(Member)
ICICI Bank

R.Ravikumar
(Member- Secretary)
RBI

Mumbai
Date: April 2, 2002

Chapter II

Standardised Checklist for conducting Computer Audit

2.1 Banking business is different from other businesses in many ways with the single important difference being banks are the custodians of the public money. Banks are intermediaries facilitating mobilization of deposits from savers and lending the same and in the process earn a reasonable spread so that they can meet the expenses involved in carrying out the intermediary business and generate adequate return for the capital providers. Banking system plays a very important role in the economic development of the country and hence always been subjected to severe controls as compared to any other industry.

2.2 Until recently, banking transactions were put through manually. However, the banking world has changed dramatically in the past ten years and thanks to the technological developments the level of computerization in banking industry has gone up manifold. Computers are extensively used to process data and to generate Management Information now. As the technology is becoming affordable, more and more players are adopting the high level of computerization for carrying out the business. Information technology is at the centre of strategic business management, delivering value to customers, fostering customer centric culture, exploring the internet channel, information and knowledge assimilation, risk mitigation and management, these elements being critical success factors in emerging markets.

2.3 We are aware of the benefits of adopting new technologies and computerization to the shareholders, management and customers. But it needs to be understood that technology changes the business processes and we are embarking on an un-chartered territory as far as controls are concerned. As Central Vigilance Commissioner said, technology is in a way like Lord Vishnu, who is described as "bhaya krita bhaya nashana". He is both the ‘creator of fear and also destroyer of fear’. So if technology can lead to frauds, it can also devise systems to check the fraud.

2.4 “Knowledge is of two kinds. We know of a subject ourselves or we know where we can find information upon it – Samuel Johnson. This quotation is appropriate for Information Technology. Even if one does not know the subject, there are many information providers. On the issue of information technology in the banking industry a lot of pioneering work has already been done. Some of the work relating to this area by RBI is indicated under:

1. Jilani Committee Recommendations: It was recommended that the Information System audit needs to be brought under Inspection Departments of Banks
2. Narasimham Committee –Second: The committee reiterated the importance of IS Audit in Banks
3. Vasudevan Committee: The committee has underlined the importance of computerization and computer resources and suggested ways to embrace it.

4. Internet Banking Committee: The report prepared by a group on behalf of RBI, has highlighted several important security issues in Internet Banking and has recommended IS Audit.
5. Working Group for Information System Security for the Banking and Financial Sector - headed by Dr. R.B.Burman, E.D: The working group has prepared a document on Information System Audit Policy and the same has been circulated among all banks by the Department of Information Technology, RBI recently. Though the document has been forwarded to IBA for necessary action, this would serve as a basic document for bank on IS audit and IS security issues.

2.5 Instructions / Guidelines issued by DBS / DBOD:

1. Inspection Manual for Banks with Computerised Accounting Systems – document prepared with the help of Coopers & Lybrand (UK C&L) for internal circulation among RBI Inspectors
2. Guidance Note on Record Maintenance – January 1998
3. Guidance note for Banks on Risks and Controls in Computer and Telecommunication Systems
4. DBOD circular on Internet Banking
5. DBS circular on EDP Audit cell to be part of Inspection & Audit Department in Banks dated June 1999

2.6 The current work:

Audit Sub Committee of the Board for Financial Supervision, while discussing the level of computerization in banks and the control over the same desired that a committee may be set up to prepare standardized checklists for conducting computer audits in different types of commercial bank branches. Hence a committee was formed under the chairmanship of Shri A.L.Narasimhan, Chief General Manager-in-Charge, Department of Banking Supervision, Central Office with participation from RBI, Institute of Chartered Accountants of India, SBI, Citi Bank and ICICI Bank.

2.7 It was felt that preparing a standardized general checklist for conducting computer audit would have the following benefits:

1. Help the Top Management understand the risks involved in IS area.
2. Be a Reference Document for carrying out IS Audit
3. Demystify the complications involved in the IS Audit process
4. Bring about standardization in IS Audit approaches so as to ensure that required care is taken
5. Help identify different risks involved in the Information Systems

2.8 Standardized checklist would be only in the nature of guidelines and banks would be free to have more elaborate checklists to conduct IS Audit suitable to the IT environment in which they operate and propose to operate. However, the issues elaborated in the checklists would give a fair idea about areas that need to be controlled.

2.9 Different levels of computerization:

Levels of computerization in the Indian Banking industry vary significantly. On the one hand centrally computerized and fully networked new private banks and foreign banks and on the other with little computerization in old private banks and PSBs are in two ends of the spectrum. However, it would be fair to clarify that there are not many banks with significant assets which would be at the lower end of the spectrum, partly due to the benefits of the technology perceived by the banking industry and the fiat issued by CVC to computerize 70 per cent of business within a target date. Competition in the industry, cutting edge technology based customer services and products, growing customer needs, RBI guidelines, guidelines issued by CVC and VRS offered by Banks are some of the factors that are forcing all the players to computerize the operations quickly and effectively. This sudden spurt naturally brings new

risks and thus there is an urgent need to document various risks involved in different levels of computerization, the controls available, the controls needed and the residual risks which the bank after careful consideration of all issues involved is ready to accept. Different levels of computerization could be

- Centrally Computerized and Fully Networked Banks
- Fully Networked Banks with distributed computing
- Banks offering Internet Banking, POS connectivity etc.
- ATMs including SWADHAN
- Local Area Networked and Wide Area Networked administrative offices
- Fully computerized branches
- Partially computerized branches
- ALPM branches
- PC based branches
- Banks at different stages of SDLC
- Corporate e-mail systems
- Off-shore data processing

2.10 Computer Audit or IS Audit?

These terms are generally not understood clearly in the industry. Computer Audit would generally mean functional audit in computerized environment and IS Audit would mean the information system audit without the functional focus. It is a common practice in many Public Sector Banks to assign the work of IS audit to regular Inspectors who do not have commensurate exposure or qualifications to carry out such audit. Growing levels of computerization in the banking industry, complexities of emerging technologies, networking, internet banking etc. necessitate proper IS security and controls in place and regular IS audits. On the functional aspect also, as most of the operations are computerized, the auditors need to necessarily carry out the audit on computer and computer audit has become day-to-day routine in banking industry.

2.11 Possible areas of audit interest in the IS environment have been broadly classified under different categories and questionnaires have been prepared under each of these categories.

2.12 It was felt by the committee that IS Audit Checklist prepared need to be platform independent and necessary platform dependent control questionnaire can be framed by the Banks themselves. Computer Audit questionnaire also should be Bank independent. On the basis of the practices followed by individual Banks they may frame Bank specific control questionnaire.

2.13 The checklists may be used in conjunction with the IS Audit policy booklet forwarded by DIT, RBI.

1 Shri Ashok Chandak was the Vice-President of ICAI when the Committee was formed. Shri R.Bupathy substituted him as the member in the Committee consequent on his election as the new Vice-President.

1. Business Strategy

1.1 Whether the business strategy is documented and business objectives have been defined and the role of IT has been clearly spelt out in the Business Strategy?

1.2 Whether information technology issues as well as opportunities are adequately assessed and reflected in the organisation's strategy, long term and short term plans.

1.3 Whether assessments are made periodically by the bank to ensure that IT initiatives are supporting the organization mission and goals?

1.4 Whether major developments in technology (hardware, software, communication etc.) are assessed for their impact on the business strategy and necessary corrective steps, wherever needed, are taken?

2. Long Term IT Strategy

2.1 Whether long term IT strategy exists and documented?

2.2 Whether the Long Term plan covers

- Existing and Proposed Hardware & Networking Architecture for the Bank and its rationale
- Broad strategy for procurement of hardware, software solutions, vendor development and management
- Standards for hardware / software prescribed by the proposed architecture
- Strategy for outsourcing, in-sourcing, procuring off the shelf software, and in-house development
- Information Security architecture
- IT Department's organizational structure
- Desired level of IT Expertise in Banks human resources, plan to bridge the gap, if any
- Strategies converted into clear IT Initiatives with a broad time frame
- IT Costs and cost management
- Plan for transition, if any

2.3 Whether the Long Term plan is approved by the Board?

2.4 Whether organization structure of IT has been made part of the IT plan?

2.5 Whether IT long-range plan is supporting the achievement of the organisation's overall Mission and Goals?

2.6 Whether a structured approach to the long-range planning process is established?

2.7 Whether the plan is covering what, who, how, when and why of IT?

2.8 Whether prior to developing or changing the long term information technology plan, management of the information services function have assessed the existing information systems in terms of degree of business automation, functionality, stability, complexity, costs, strengths and weaknesses in order to determine the degree to which the existing systems support the organisation's business requirements?

2.9 Whether organizational model and changes to it, geographical distribution, technological evolution, costs, legal and regulatory requirements, requirements of third-parties or the

market, planning horizon, business process re-engineering, staffing, in or out sourcing etc. are taken into account at the time of planning process?

2.10 Whether plan refers to other plans such as the organizational plan and the information risk management plan?

2.11 Whether process exists to timely and accurately modify the long range IT plan taking into account changes to the organisation's plan and in business and information technology conditions?

2.12 Whether a security committee, comprising of senior functionaries from IT Department, Business Group, IT Security Department and Legal Department is formed to provide appropriate direction to formulate, implement, monitor and maintain IT security in the entire organisation?

3. Short Range IT Plans

3.1 Whether long-range IT plans are converted to short-range IT plans regularly for achievability?

3.2 Whether the IT Short range plan covers the following

- Plan for initiatives specified in the Long range plan or initiatives that support the long range plans
- System wise transition strategy
- Responsibility and plan for achievement

3.3 Whether adequate resources are allocated for achieving the short-range plans?

3.4 Whether short-range plans are amended and changed periodically as necessary in response to changing business and information technology conditions?

3.5 Whether assessments are made on a continuous basis about the implementation of short range plans?

3.6 Whether clear-cut responsibilities are fixed for achieving the short range IT Plan?

4. IS Security Policy

4.1 Whether a well-documented security policy is available?

4.2 Whether Inventory of IT assets is made part of the policy? Whether inventory of IT assets is kept at branch / office level?

4.3 Whether policies related to IT activities are listed in the security policy?

4.4 Whether the policy takes into account the business strategy / plan for the next 3 – 5 years?

4.5 Whether the policy takes into account the legal requirements?

4.6 Whether the policy takes into account the regulatory requirements?

4.7 Whether the policy is approved and adopted by the Board of Directors / Top Management?

4.8 Whether the policy is communicated to all concerned and is understood by them?

4.9 Whether the following major security areas are covered in the policy ":

- PC and LAN, MAN and WAN security
- Physical Security to IS establishments
- Handling of confidential information
- Handling of security incidents
- Privacy related issues for outside entities
- E-mail security
- Application security
- Interface Security
- Password Security
- Operating system security, web site security
- Database security
- Anti virus and piracy policy
- Archived and Backed up data security
- Procedures for handling incidence of security breach
- Disaster Recovery Plan
- Use of cryptology and related security
- Persons responsible for implementing security policy and consequence for willful violation of the Security Policy

4.10 Whether a review process is in place for reviewing the policy at periodic intervals and / or on any other major event?

5. Implementation of Security Policy

5.1 Whether documented security policy is made available to all the levels of users to the extent relevant to them?

5.2 Whether continuous awareness programmes are conducted for security awareness?

5.3 Whether the role of Information Security Officer with responsibilities for implementation of the Security Policy has been assigned?

5.4 Whether detailed procedures for each policy statement are developed?

5.5 Whether suitable methodologies are adopted for implementation?

5.6 Whether suitable security tools are selected for implementation?

5.7 Whether the roles of the implementers are clearly defined?

5.8 Whether the budgetary allocation for implementation of IS security is assessed and documented?

5.9 Whether periodic security audits are carried out?

5.10 Whether on the basis of audit reports or any other vital information suggestions for updating the security policies are conveyed to the right / appropriate management?

5.11 Whether management demonstrates adherence to the Security Policy?

5.12 Whether new entrants are given adequate exposure to the security policy?

5.13 Whether in case breaches of security policy the root cause is analysed and preventive and corrective actions are taken?

5.14 Whether incidence-reporting procedures have been followed?

5.15 Whether the Information Security Officer is made responsible for reporting non-compliance with the approved policy and incidents of security breaches to the Top Management, and to initiate and effect corrective action?

6. IS Audit Guidelines

6.1 Whether a documented and approved IS Audit guidelines are available?

6.2 Whether IS audit guidelines are consistent with the security policy?

6.3 Whether the IS audit responsibilities have been assigned to a separate unit which is independent of IT Department?

6.4 Whether periodic external IS audit is carried out?

6.5 Whether independent security audit is conducted periodically?

6.6 Whether contingency planning, insurance of assets, data integrity etc. are made part of external audit?

6.7 Whether vulnerability and penetration testing were made part of external audit?

6.8 Whether the major concerns brought out by previous Audit Reports have been highlighted and brought to the notice of the Top Management?

6.9 Whether necessary corrective action has been taken to the satisfaction of the Management?

6.10 Whether adequate training facilities are provided to IS audit teams so as to enable them to conduct audits effectively?

6.11 Whether IS audit team is encouraged to keep themselves updated?

6.12 Whether IS auditors exchange their views and share their experiences internally?

7. Acquisition and Implementation of Packaged Software

Procurement and implementation of packaged software has various stages in the entire process. The information system auditor (SA) has to familiarize himself with the policies and practices of the bank with regard to software procurement and implementation. The IS Auditor should have prior discussion with the IT Department and should gain the following knowledge before commencing audit work of this area

- IT Infrastructure and environment in the Bank
- Resources available in the IT Department of the Bank
- Software Products procured and implemented during the period
- Status of the implementations
- Problems if any faced by the users after implementation
- Errors noticed in processing transactions in the procured system
- Any Errors resulting in financial loss, regulatory / compliance issues, serious customer complaints etc.

Note : This check list does not address commercial consideration for which regular audit guidelines have to be applied

This checklist is divided into the following Areas

(a) Requirement Identification & Analysis
(b) Product & Vendor Selection Criteria
(b) Vendor Selection Process
(c) Contracting
(d) Implementation
(e) Post Implementation Issues

(a) Requirement Identification and Analysis

7.1 Is there an annual plan covering areas requiring computerisation approved by Top Management?

7.2 Is plan in line with the Banks overall IS Strategy?

7.3 Has a functional manager or a committee been identified as responsible sponsors for an area requiring computerisation?

7.4 Have the costs of computerisation been budgeted and included in the overall IT Budget of the Bank?

7.5 Has a detailed plan been made by the IT Department, clearly providing the date of commencement, activities involved, target date of final implementation and estimated costs for each area identified?

7.6 Has this plan been approved by the Sponsor?

7.7 Has a document been prepared clearly detailing the following requirements:

Functionality

In case of replacement, the problems faced in the existing system and need for replacement

Performance

Security

Operations Risk Mitigation

Acceptance Criteria for the System

Changes in the operating procedures required to implement the proposed system and persons responsible and plan for effecting the changes

Transition / Migration from existing to proposed plan for a smooth transition

Interface requirement with Other Computer Systems

7.8 Has the requirements been graded as Vital, Essential and Desirable?

7.9 Has the Sponsor approved the requirement document?

(b) Vendor Selection Criteria

7.10 Has the Requirements Document been translated clearly into product acceptance criteria ? Has Acceptance Criteria been classified into:

'Show Stoppers'

'Allowable Customisations'

'Desirable positive features'

7.11 Do the IT Department have a technology standard for product selection?

7.12 Does the Technology standard cover:

- Architecture
- Open Database standards
- Interfaces and API Standards
- Security Standards

7.13 Are the Product Selection criteria consistent with the IT platform of the Bank? Does the Bank have clearly laid down and approved guideline for selection of product vendors?

7.14 Does the Vendor Selection guideline address the following:

- Market Presence
- Years in operation
- Technology alliances
- Desired size
- Customer base and existing implementation
- Support
- Possibilities of partnership or strategic alliance
- Source code availability
- Local Support in case of foreign vendors

7.15 Has the selection criteria been decided by the IT Department in consultation with User Departments?

7.16 Has the Sponsor approved the Selection Criteria?

7.17 Does the policy of the bank permit beta-site installations? If yes are criteria for selection distinctly different from regular guideline?

7.18 Does the IT Department use scoring model for evaluating the products and vendor?

7.19 Do the scoring criteria consider the following factors:

- Extent of customization and work around solutions
- Security Features
- Technology fit
- Performance & Scalability

- No. of installations
- Existing customer reference
- Cost
- Vendor Standing

(c) Vendor Selection Process

7.20 Does the IT Department have a system to identify potential vendors for an area (such as subscription to magazines; rating reports and reports of specialized agencies such as Gartner, IDC, Data Quest etc.,)

7.21 Are reports of specialized independent rating agencies used for short listing Vendors?

7.22 Does the Bank have a system of floating formal RFP (Request for Proposal) for systems with estimated budget exceeding a certain amount?

7.23 Is there a core team comprising of personnel from IT Department, Functional Departments and Internal Audit Department in charge of vendor selection and implementation?

7.24 Is the process of selection for each area approved by the Sponsor?

7.25 Are Meetings of the Core Team documented?

7.26 Does Team use prepared check lists for

(a) Product Evaluation
(b) Site Visits
(c) Customer Reference

7.27 Is final evaluation and selection fully documented and approved by the Sponsor?

7.28 Does the document clearly reflect the rationale used for the selection?

(d) Contracting

7.29 Does the bank have approved terms and conditions for Product Licensing Agreements?

7.30 Do the Licensing terms contain:

a) Escrow mechanism for Source codes
b) Facilities for minor customisation
c) Maintenance and Upgrades

7.31 Does the Bank have a Service Level Agreement with Product Vendors for Support and Maintenance?

7.32 Where the contract is entered with a Distributor or Reseller is there a commitment to ensure that the actual owner would support the Bank in case of relationship between the owner and the reseller breaks?

7.33 Does the contract clearly segregate duties and responsibilities of the Bank and the Vendor?

7.34 Does the contract include a clause to protect the Bank from the Vendor using the bank data?

7.35 Does the contract clearly specify the product base lines?

(e) Implementation

7.36 Is gap analysis between the requirement and the selected product carried out and documented?

7.37 Does this document act as the basis for further implementation plans?

7.38 Does the Bank's policy provide for parallel run of previous system during the implementation period?

7.39 Is there an agreed plan for implementation? Has the plan been approved by the Sponsor, Vendor and IT Department?

7.40 Does the implementation plan clearly identify product customisation requirements, user acceptance criteria and test for such customisation?

7.41 Does the implementation plan address data migration from previous systems?

7.42 Does the implementation cover the following:

a) User Departments' involvement and their role
b) User Training
c) System Administration Training
d) Acceptance Testing
e) Role of Vendor and period of Support
f) Required IT Infrastructure plan
g) Risk Involved and actions required to mitigate risks

7.43 Does the responsibility for accuracy of key parameters / Static Data rest with the functional department?

7.44 Is there a list of areas which will be controlled by the Vendor during the implementation phase?

7.45 Does Bank have a test environment to simultaneously allow familiarisation during the implementation process? Have errors identified during the implementation phase been documented and the root cause of the errors analysed and confirmed by the Software Vendor?

7.46 If there are bugs and errors due to design flaws, are they escalated to higher levels in Software Vendors' organisation and the bank?

7.47 Is Test packs developed by user groups for testing customisation delivered by the vendor?

7.48 Is there a clearly identified data integration strategy during customisation period? (If customisation involves additional elements of data to be captured)

7.49 Is the result of testing properly documented?

7.50 Are necessary changes to System documents carried out on customization?

7.51 Are all following documents handed over by the Vendor?

- System Documentation covering Design and Program Documentation
- Data Dictionary
- Installation Manual
- User Manual
- Trouble Shooting

7.52 Does the IT Department have a proper archival system for these documents?

7.53 In cases where source code is given by the Vendor, has the IT department done a technical conversion and issued a confirmation of satisfactory compilation / performance?

7.54 Is there a system to issue formal Acceptance Certificate signed off by User Department, IT Department and the Sponsor?

(f) Post Implementation Issues

7.55 Has the IT Department taken the required consequential action for Back ups, Disaster Recovery and Performance Tuning?

7.56 If Source codes are delivered, are the source codes base lined as per IT Department Procedures?

7.57 Has the IT Department in consultation with User Department worked out Database Controls?

7.58 Has IT Department introduced a system to track problems reported by users, escalation to vendor and their resolution?

7.59 Is there a system of measuring vendors' support with the agreed service levels?

7.60 Is there an identified System Administrator who is responsible for managing access to the system, back up and ensuring data base controls?

8. Development of software – In-house and Out-sourced

Audit framework for Software developed in-house

Software Audit Administration

8.1 Is the software audit (SA) conducted using pre-designed formats at three levels viz.

a) Program Level,
b) Application Level and
c) Organization Level

8.2 Has IT department adopted any Standardised quality processes such as ISO, SEI CMM etc., for Software development?

8.3 Has Non compliance reported in such quality audit are properly attended to and rectified?

8.4 Is there a system in place to reveal the outcome of the audit to the staff of the Bank at respective levels?

8.5 Whether a structure is in place for effective Software Audit so that reliable results can be obtained?

Software Audit Process

Audit at Program Level

8.6 Are the programs developed by drafting the formal specifications, defining scope, application, input data elements, output requirements, process work flow etc.?

8.7 Is software tested for quality assurance?

8.8 Is quality assurance team different from development team?

8.9 Are data / test results preserved for future reference?

8.10 Are there temporary patches developed by just copying a few set of legacy programs? If so, are they tested properly before deployment and limitations and conditions, which such programs cannot handle, is communicated to users and appropriate control procedures are put in place?

8.11 Do all the program source codes contain a Title area, specifying the author, date of creation, last date of modification and other relevant information?

8.12 Are there adequate input validation checks built into data entry programs?

8.13 Whether the following manuals are prepared?

Systems operations / Installation Manual

User Manual

8.14 Are there well-established testing procedures? Does the testing procedures cover

- What, When and How to Test?
- Positive (Test done by processing valid data and checking if the results are accurate) and Negative Testing? (Test done by processing invalid data and checking if the program generates necessary error messages)
- Performance and scalability?
- Recording and maintaining test results?

8.15 Whether parallel testing at a few pilot installations done after completing pre-implementation testing?

8.16 Whether programs successfully implemented have passed the test for accuracy of outputs generated?

8.17 Whether the source code location with ownership for future up-gradation is well established?

8.18 Whether every patch / update is authorized by a competent authority?

8.19 Whether the development consider security requirement as per approved security policy?

Audit at Application Level

8.20 Are operational controls such as distinct user passwords are in place and are enforced?

8.21 Whether necessary 'Regulatory Compliance' requirements have been taken into account by the user?

8.22 Whether SRS has taken into account the Error / Fraud / Disclosure / Interruption / Organisational Risks etc.?

8.23 Whether input / output controls are in place?

8.24 Are validation controls are in place, viz. Field / Transactions / File with appropriate error reporting?

8.25 Are appropriate data classifications with security in place, viz. Read only for users, Read / Write for authorized persons?

8.26 Is audit trail built into the systems?

8.27 Does the system provide for ‘exception reporting’ ?

8.28 Whether adequate firewalls set up to ensure that any outside access being provided is limited in scope ad does not intrude on sensitive data areas?

8.29 Whether user acceptance is recorded along with test plan data / test data / test results for future reference?

8.30 Whether the user sign off has been obtained?

Audit at Organisational Level

8.31 Is updated organizational chart being kept?

8.32 Are the duties of developers and operators of the system distinctly segregated?

8.33 Is job rotation in place?

8.34 Whether software implementation plan has been approved by the controlling authority?

8.35 Whether provision has been made for maintenance of software library?

8.36 Is there a system in place for software distribution?

8.37 Are error reporting and control mechanisms in place?

8.38 Is there a system for post completion ‘Review Audit’?

8.39 Is there a a standard and secure procedure for up-keep of source / object code?

8.40 Are security controls including Disaster Recovery in place?

8.41 Is the data conversion audited?

8.42 Are all changeovers from one system to another system authorized by a competent authority?

8.43 Are the training requirements for users properly identified?

8.44 Is the DRP in place at all operating offices?

8.45 Are documentations available at operational stage to facilitate formal changeover of jobs?

Audit framework for Software Outsourcing

8.46 For software development outsourcing, are there laid down criteria for selection of vendors?

8.47 Whether formal outsourcing strategy for necessary interface with the vendor is in place?

8.48 Is the outsourcing activities evaluated based on the following practices?

What is the objective behind Outsourcing?

What are the in-house capabilities in performing job?

What is the economic viability?

What are the in-house infrastructure deficiencies and the time factor involved?

What are the Risks and security concerns?

What are the outsourcing arrangement and fall back method?

What are arrangements for obtaining the source code for the software?

8.49 Is there formal approval system in place from the Head of the user department?

8.50 Does the user department representative 'Expert Officer' visit the vendor's premises for reviewing the capability and quality of software development activities?

8.51 Does the vendor present the progress of software development at periodic intervals?

8.52 Is there a formal product hand over and project completion system in place?

8.53 Is there an Agreement entered by the Bank with the Vendor for completion of the software development in time. Whether any penalty clause exists for delayed completion of work?

9. Physical Access Controls

9.1 Whether there is a policy regarding physical access control and is a part of the security policy of the organisation?

9.2 Whether there is a mechanism to review the policy regularly?

9.3 Whether the policy on the following are appropriate:

- Lay out of facilities
- Physical and Logical Security
- Safety
- Access
- Maintenance
- Signage
- Visitors
- Health
- Safety and environmental requirements
- Entrance and exit procedures
- Regulatory requirements
- Legal requirements

9.4 Whether the Information System facility located in a place which is not obvious externally?

9.5 Whether the facility is located in least accessible area or / and access is limited to approved personnel only?

9.6 Whether the physical access control procedures are adequate for employees, vendors, equipment and facility maintenance staff?

9.7 Whether 'Key' management procedures and practices are adequate? Whether review and updates are carried out on a least access needed basis ?

9.8 Whether the access and authorization policies on the following adequate?

Entering / Leaving

Escort

Registration

Visitor passes

Surveillance cameras

9.9 Whether the policies laid down are implemented?

9.10 Whether periodic review of access profiles is carried out?

9.11 Whether revocation, response and escalation process in the event of security breach appropriate?

9.12 Whether security for portable and off-site devices adequate?

9.13 Whether control of visitors adequately addressed? Whether issues like registration, pass, escort, logbook for check in and check out are handled properly?

9.14 Whether fire prevention and control measures implemented are adequate and tested periodically?

9.15 Whether computing facilities are situated in a building that is fire resistant and wall, floor and false ceiling are non-combustible?

9.16 Whether smoking restriction in computing facilities are in place?

9.17 Whether smoke / heat-rise detectors installed and connected to the fire alarm system?

9.18 Whether fire instructions are clearly posted and fire alarm buttons clearly visible? Whether emergency power-off procedures are laid down and evacuation plan with clear responsibilities in place?

9.19 Whether fire drill and training are conducted periodically?

9.20 Whether computing facilities are located above ground level? Whether water leakage, seepage etc. are prevented?

9.21 Whether air-conditioning, ventilation and humidity control procedures in place, tested periodically and given adequate attention

9.22 Whether security awareness is created not only in IS function but also across the organisation?

9.23 Whether physical security is continually addressed and whether physical security is ensured at suppliers facilities also in cases where organisation's' assets either physical or data are processed at supplier's facilities?

9.24 Whether UPS is available? If so, is it covered under maintenance?

9.25 Whether alternate or re-routing telecommunication lines are available?

9.26 Whether alternative water, gas, air-conditioning and humidity resources are available?

9.27 Whether all access routes are identified and controls are in place?

9.28 Whether the computer room is locked and access is restricted?

9.29 Whether appropriate holidays and vacation are availed by the IT staff?

9.30 Whether hazardous commodities are not stored in the IS area?

9.31 Whether appropriate access controls like password, swipe card, bio-metric devices etc. are in place and adequate controls exist for storing the data / information on them?

9.32 Wherever access to the I S facility is enabled through ID cards / badges, etc., are there controls to ensure that the issue and re-collection of such access devices are authorised and recorded.

9.33 In case of outsourced software, whether all maintenance work is carried out only in the presence of / with the knowledge of appropriate bank staff?

9.34 Based on criticality of the IS facility, are there video surveillance equipments to monitor the movements of the personnel inside the facility? If so, check whether continuity of video recording is ensured.

9.35 Whether access violations are recorded, escalated to higher authorities and appropriate action taken.

10. Operating System Controls

Adherence to licensing requirements

10.1 Whether the Branch / Office holds the original license from the Head Office / Vendor for using the operating system software?

10.2 Whether the original Operating System Media supplied by the vendor is available in the Branch / Office?

10.3 Verify all the manuals and user guides provided by the vendor at the time of supply of the system and ensure whether all are physically available. Ensure that proper library records are maintained by the Branch / Office for all the manuals / books received along with the package.

10.4 Ensure whether the number of licenses used in the Branch / Office is less than or equal to the number of user licenses mentioned by CPPD / Vendor in the license

Version Maintenance and application of patches

10.5 Verify the system configuration such as Memory, Clock speed, Hard Disk size, OS version, etc. and ensure that they are as per order or terms stipulated by CPPD / IT Dept. at the time of procurement.

10.6 Ensure that the latest OS version is running at the site. Check whether latest updates / patches released by the OS vendor have been applied.

Network Security

10.7 Check if the system being audited trusts other hosts for providing logon access to similar user accounts (same user account in the system being audited and the host system) in both the systems without supply of password. If so, ensure that it has been implemented in accordance with IT / CPPD guidelines only.

10.8 Check if remote logon is enabled and if so, whether it is as per the guidelines of CPPD / IT Department. Ensure that the users logging on from remote locations are identifiable by terminal IDs / IP addresses.

10.9 Check if remote logon through services such as ftp, telnet, etc. is disabled. If not, ensure that the same has been implemented as per IT security policy of the Bank.

User Account Maintenance

10.10 Each and every user ID in the operating system level should have been created only after specific approval of the Branch Manager / Department head in writing on a request form signed by the respective user. Verify whether such approval is in place for all the active user IDs.

10.11 Apart from the approved request forms, the Branch / Office should be maintaining a user profile register with details such as,

- Employee Name
- Designation
- Employee Number
- Date of joining the Branch / Office
- User ID allotted
- Date of creation of user ID
- Date of deletion of user ID
- Signature of the user
- Initials of the DBA
- Initials of the BM

Verify whether the above mentioned register is maintained. All the entries in the register should be accounted for in the list of active user IDs obtained from the operating system.

10.12 Check that with the exception of reserved user accounts created for the internal use of the operating system, RDBMS, Application system, etc., all other user accounts are uniquely identifiable by the respective user's personal name. In other words, generic user accounts, which cannot be attributed to any individual, should not be allowed. Verify this and comment.

10.13 Check the operating system user IDs which have security equivalence to Super User and ensure whether they are permissible as per CPPD / IT Department guidelines.

10.14 Check whether all the user IDs are protected with passwords.

10.15 With the exception of Super User account, check whether all default system login accounts are disabled. In other words, ensure whether all default vendor accounts shipped with the Operating System have been disabled. This should be checked after each upgrade or installation.

10.16 Check the list of active user groups and ensure that general users are not members of sensitive / privileged user groups which have higher privileges.

Logical Access Controls

10.17 Ensure that access to operating system command prompt is disabled for general users in the Branch / Office.

10.18 If some or more of the system administration related activities are driven through a menu-based utility assigned to any user ID, which is privileged, ensure that such ID(s) cannot be used to bypass login security and access the command prompt.

10.19 Ensure that the file pertaining to each user containing login parameters cannot be modified by the respective user.

10.20 Ensure that any user other than the Super User cannot modify the system activity log file.

10.21 Check whether access rights to system files, application executable program files, application data files, utilities, application parameter files, system/database configuration/initialization files, etc. have been adequately controlled to allow read / write / execute / modify, etc. as the case may be to appropriately authorised users on need to know, need to do basis.

10.22 Obtain a list of world writable (directories / folders with access to every user) directories / folders in the system and ensure that they have been set only in accordance with IT / CPPD guidelines.

10.23 Verify the access rights settings for the users' home directories and ensure that they are not owned by any ID other than the actual user. Also, ensure that user's home directory cannot be accessed by any other user.

System Administration

10.24 Ensure that the facility to logon as Super User is restricted to system console for security reasons.

10.25 Check the password definition parameters included in system and ensure that minimum password length is specified according to the IT security policy of the Bank (ideally, atleast 6 characters).

10.26 Ensure that the maximum validity period of password is not beyond the number of days permitted in the IT Security policy.

10.27 Check whether the parameters to control the maximum number of invalid logon attempts has been specified properly in the system according to the security policy.

10.28 Check whether password history maintenance has been enabled in the system to disallow same passwords from being used again and again on rotation basis.

10.29 Verify if the parameters to control the password format has been properly set according to security policy of the Bank.

10.30 Verify the parameters in the system to control automatic log-on from a remote system and ensure whether they have been properly set according to security policy.

10.31 Verify the parameters in the system to control the number of concurrent connections a user can have simultaneously from different terminals and ensure that it is restricted as per CPPD / IT Department guidelines.

10.32 Examine the terminal inactive time allowable for users and verify if the time set is in accordance with the guidelines.

10.33 If minimum password validity period is not set properly, verify the latest date of change of privileged passwords including Super User and ensure that the password is not too old, in any case not older than a month.

10.34 Check whether automatic logging of user activities is enabled.

10.35 Check for unexpected users logged on to the system at odd times.

Maintenance of sensitive user accounts

10.36 Ascertain as to who is the custodian of sensitive passwords such as Super User and verify if he/she is maintaining secrecy of the password, whether he/she has preserved the password in a sealed envelope with movement records for usage in case of emergency.

10.37 From the log file, identify the instances of use of sensitive passwords such as Super User and verify if records have been maintained by the Branch / Office with reason for the same. Ensure that such instances have been approved by CPPD / TBC Group / IT Department and whether Branch Manager, Password Custodian and DBA have signed the record.

10.38 From the log file, identify the instances of unsuccessful logon attempts to Super User account and check the terminal ID / IP address from which it is happening. Check if appropriate reporting and escalation procedures are in place for such violations.

11. Application Systems Controls

The application system before being implemented has to be reviewed by the auditor if various controls suggested by Users are incorporated in the application system. The various controls, which have to be included in the system are as follows:

- Logical Security
- Input Controls
- Processing Controls
- Output Controls
- Authorisation Controls
- Interface Controls
- Data integrity / File continuity Controls

Logical Access Controls

11.1 Does the software allow creation of user-IDs in the same name more than once?

11.2 Does the software encrypt the passwords one way and store the same in encrypted form?

11.3 Does the software display the password as it is keyed in?

11.4 Does the software lock the user-ID if it is used for 3 unsuccessful times to logon to the system?

11.5 Does the software force the User to change the password at set periodical intervals?

11.6 Does the software maintain password history i.e., does not allow the same password to be used again on rotation basis?

11.7 Is there any audit trail for the maintenance of User profiles?

11.8 Does the software have provision to create and maintain user-IDs based on users' designations and positions held?

11.9 Can DBA change other's password? If so is it reflected in the audit trail?

11.10 If a user-id record is deleted, does the software delete it physically or logically? Does the software capable of producing a report of logically deleted User-IDs?

11.11 Does the software have provision to restrict different menu options to different user-IDs based on user level (based on designation / powers, etc.)?

11.12 Does the software have provision for defining access rights to users such as, Read Only, Read and Write, Modify, Delete, etc.?

11.13 Verify who can do the User Profile Maintenance? Does the system give facility to general users also to do user profile maintenance?

11.14 Does the software tag each and every transaction with the user-IDs of maker and checker?

11.15 Does the software allow the same user to be both maker and checker of the same transaction? If so, does the software produce an exception report of transactions with same maker and checker IDs?

11.16 Are the User-IDs reflected in the contents of the report printed?

11.17 Does the software allow automatic logical deletion of inactive users after certain period of time?

11.18 Does the system maintain password length to be of minimum 6 or 8 characters or as indicated in the password policy?

11.19 Can the user-IDs be created without passwords?

11.20 Does the system limit the maintenance of system control parameters to privileged user level having sufficient authority only?

Input Controls

11.21 Whether each transaction is recorded in such a way that it can be subsequently established that it has been input (e.g., Tran ID etc)?

11.22 Does the software have controls to ensure that all recorded transactions are,

.22.1 Input to the system and accepted once and only once.

.22.2 If transactions are rejected, they are reported.

11.23 Are there adequate procedures to investigate and correct differences or exceptions identified? Are there adequate procedures to investigate and if necessary, correct the following: -

- Missing and possible duplicate transactions disclosed by the input control
- Rejected items

11.24 If corrections are made to rectify differences, exceptions, duplicate transactions, missing transactions and rejected items, are they approved (e.g., maker/ checker, exception report, etc.)?

11.25 If the input of data is through batch upload, does the software have controls to ensure that all the entries in the batch have been uploaded without any omission/ commission (e.g., reconciliation of control totals, etc.)?

11.26 Does the software have adequate controls to ensure that, data have been accurately input (e.g. range checks, validity checks, control totals, etc.)

11.27 Verify the controls to ensure compatibility of data when they are input at two or more modules and are correlated. (e.g. if the customer category in customer master is stated as "Staff", the rate of interest in the account master for the same customer should have appropriate code applicable to staff and system should not allow other codes).

11.28 Verify the consistency/concurrency of user inputs, if two users are accessing the same record at the same time.

11.29 Verify if the inputs can be captured for various conditions. (e.g. if signatures can be captured for single A/c, Joint A/c etc).

11.30 Verify the controls over system-generated transactions through user processes (e.g. verification of outputs containing system generated transactions and authentication by branch officials).

11.31 If user controls are relied upon to ensure the controls over complete and accurate input of data, are these controls adequate and operative continuously?

Processing Controls

11.32 Does software have adequate controls to ensure that all transactions input have updated the files?

11.33 If user controls are relied upon to ensure the controls over complete and accurate update of files with data, are these controls adequate and operative continuously?

11.34 Are there adequate procedures for investigation and correction of differences or exceptions identified by the controls over update for completeness and accuracy?

11.35 Are such corrections approved?

11.36 List out the events that cause the transaction to be generated (e.g. input of a parameter such as a date, attainment of a condition, etc.), the key data used as a basis for the generation, and the programmed procedures that perform the generation. (e.g., in the interest calculation process, generally, the user will run the interest run job and the system will take the customer balances (key data) and apply interest rates (key data) and debit/credit the interest. The program, which performs these activities, should be logically sound so that no processing errors are introduced).

11.37 For the key data outlined above, are there adequate controls to ensure that the key data used as a basis for the generation of data are complete and accurate?

11.38 Where applicable, whether the key data is authorised by appropriate level of users and kept secure?

11.39 For the programmed procedure that generates the data, if user controls are relied on to check the accuracy of the generation process, are these controls adequate?

11.40 Are there adequate procedures to investigate and correct any differences or exceptions identified by the controls over the completeness and accuracy of generation? Are the corrections approved?

11.41 Is there any restart facility for batch jobs if they terminate abruptly? Are there controls to ensure that no errors are introduced during restart?

11.42 Is the User-ID of the person who executes the batch job embedded in the transactions?

11.43 If the process has to be done only once, does the software ensure that the process is not executed more than once?

11.44 Is there any day begin, day end process? If so, are these processes logically sound to carry out the designed objectives completely and accurately?

11.45 Are the transactions for the day identifiable?

11.46 Does the software ensure sequencing of processes? i.e., does the software ensure that processes are not initiated out of sequence.

11.47 If certain processes are compulsory, does the software ensure that all such processes are completed before triggering the day end process?

11.48 Verify if there is an event log for the batch processes.

11.49 Verify if the application is able to handle processing at peak times (e.g. is the application capable of handling progressively increasing volumes).

11.50 Verify if software maintains audit-trail to uniquely trace any modification/ deletion/addition with user-ID.

11.51 If updates occur in more than one file or table, if the process interrupts, verify if there is a roll back.

11.52 Verify if the application maintains adequate control over security items such as DDs / Pay Orders / Branch advices, etc.? Are they reconciled and exceptions identified and reported?

Output Controls

11.53 Verify the format, contents, accuracy and utility of the reports generated by the system.

11.54 Verify if there is any provision for generating exception transactions statement from the system.

11.55 If the output has more number of pages and if printing is interrupted, is there any provision to restart the printing from that page.

11.56 Verify if outputs can be viewed/generated by users only on need to know basis. In other words, check whether outputs cannot be generated by all and sundry users in the system.

11.57 Check the controls exercised by the user (Branch / Office) on the generation, distribution, authentication and preservation of computer outputs and comment on the adequacy of the same.

11.58 Check whether the application is keeping adequate controls over computer generated outputs lying in print queue / spool.

11.59 Does the output contain key control information necessary to validate the accuracy and completeness of the information contained in the report such as last document reference, period, etc.?

Interface Controls

11.60 If the data has to be transferred from one process to another process, verify if no manual intervention is possible and no unauthorised modification to data can be made.

11.61 Verify the mode of transfer of data from one process to another i.e. through floppy or through mail.

11.62 Verify the effect when one process is down and the interface is working

11.63 Is there a periodic system of ensuring consistency of data from process from which it is transferred to the process to which it is transferred?

Authorisation Controls

11.64 If the transaction is authorised by software itself under specific conditions, are the programmed procedures logically sound to ensure that all authorisations take place as expected only.

11.65 Does the software prevent the same user from performing both the functions of entering a transaction and verifying the same?

11.66 If transactions are authorised manually, are there controls to ensure that a) they are properly authorised by an independent and responsible official and b) no unauthorised alterations are made to authorised transactions?

11.67 If manually approved transactions are authenticated by the input of a password, are passwords adequately controlled?

11.68 Do access rights reflect the appropriate authority limits?

11.69 If the transaction is identified by the system as requiring supervisory approval and is, therefore, routed to a queue file pending review and release by a responsible official, are the procedures for identifying 'items needing approval' adequate to identify all such transactions?

Data Integrity / File Continuity Controls

11.70 Whether hash total is used to verify the continued integrity of data? Is the total of the items on data file regularly reconciled to an independently established total (e.g. agreement to a manual control account or computer agreement to a control record) on a suitable timely basis to ensure that there is no tampering of data.

11.71 Are there adequate procedures to investigate and correct differences disclosed by the above-mentioned reconciliation.

11.72 Verify if the entire record after commit can be physically deleted (it should not be allowed).

11.73 If the software keeps record of security items, are there adequate controls to ensure the complete and accurate recording of security items in the system?

11.74 Are the programmed procedures, which utilise the security items in the system, logically sound so that there are no errors?

11.75 Are all asset movements supported by suitable written authorisations?

12. Database Controls

It is important to ensure the following with reference to databases:

- Database is physically secure and free of any corruption
- Access to the database is restricted and permitted only to authorized personnel
- Referential Integrity of the data is ensured at all times
- Accuracy of the contents of the database is verified periodically
- Database is also technically verified periodically, in terms of storage space, performance tuning and backup
- Backups of the database are periodically retrieved and ensured that they are in order

This checklist is divided into following areas

- Physical access and protection
- Referential Integrity and accuracy
- Administration and House Keeping

Physical access and protection

12.1 Is there a list of databases with the names of administrators which the bank recognizes:

(a) Mission Critical Systems such as Internet Banking, Core Banking etc., ATM Base 24 Database

(b) Essential Systems such as Credit Card Processing Systems (Which operate on the near online mode)

(c) Reporting Systems such as Data Warehouse, EIS Reporting

12.2 Is there joint responsibility of the user department and the IT Department for administration of mission critical databases?

12.3 Does IT Department identify and segregate hardware hosting these databases and whether these hardware resources have been year marked?

12.4 In case if the same hardware is used at branches or other locations whether there is clear partition between application area and data area?

12.5 Does the IT Department have a laid down standards / conventions for database creation, storage, naming and archival?

12.6 Are Database administrators at responsible levels in the bank?

12.7 For database access, is the OS level file and directory permissions restricted as required for the application?

12.8 Are users denied access to the database other than through the application?

12.9 Whether use of triggers and large queries monitored to prevent overloading of database and consequent system failure?

12.10 Are direct query / access to database restricted to the concerned database administrators?

12.11 Are all vendor-supplied passwords to the default users changed? Have all demo user and demo databases removed?

12.12 Are there controls on sessions per user, number of concurrent users etc?

12.13 Is creation of users is restricted and need based? Are the rights granted to various users reasonable and based on requirement?

12.14 Is the database configured to ensure audit trails, logging of user sessions and session auditing?

12.15 Does the administrator maintain a list of batch jobs executed on each database, severity of access of each batch job and timing of execution?

12.16 Are Batch Error Logs reviewed and corrective action taken by the Administrator periodically?

12.17 Is there a separate area earmarked for temporary queries created by power users or database administrator based on specific user request?

12.18 Are temporary sub databases created removed periodically or after the desired purpose is achieved?

12.19 Does the design or schema of all tables / files in database contain fields for recording makers, checkers and time stamp?

12.20 Are database administrators rotated periodically?

12.21 In cases where customer data is provided to external service providers does the bank have confidentiality undertakings from these service providers?

Referential Integrity and Accuracy

12.22 Are there standard set of database control reports designed in consultation with the user department for ensuring accuracy and integrity of the databases?

e.g.:

a) Total of transactions and balances;

b) Record Counts

c) Hash Totals

12.23 Are these reports run directly from the back end database periodically and the results both positive and negative are communicated by the Administrators to Senior Management Personnel?

12.24 Are these reports run periodically and taken directly by the User Department themselves to ensure accuracy?

12.25 In case of automated interface between systems is there a system of reconciliation between the source and receiving system for critical information?

12.26 Is there a system of periodic reconciliation between Sub databases and the GL Database of the bank?

12.27 In cases where data is migrated from one system to another has the user department verified and satisfied about the accuracy of the information migrated?

12.28 Is there a formal data migration report?

12.29 Are there entries directly made to the back end databases? If they are made under exceptional circumstances, is there a system of written authorization?

12.30 If entries in the database are updated / deleted due to any exceptional circumstances (e.g. during trouble shooting, etc.), are they approved in writing and recorded?

Administration and House Keeping

12.31 Does the System Administrator periodically review the list of users to the database? Is the review documented?

12.32 Are inactive users deactivated?

12.33 Is there back up schedule?

12.34 Are databases periodically retrieved from the back up in test environment and accuracy ensured with the physical environment?

12.35 Are senior personnel from the user department involved in testing backup retrieval?

12.36 Is there periodic purging / archival of databases?

13. NETWORK MANAGEMENT

PROCESS

13.1 Is there an Information Security guidelines document, which defines the minimum configuration for any device/link on the bank's network, including levels of encryption?

13.2 Are all platforms/links/devices in compliance with the guidelines? If not, has an appropriate level of management reviewed the non -compliant parts of the network to ensure that the risk levels are acceptable?

13.3 For all items supported by external vendors, does the vendor or the manufacturer verify that all cryptographic functions in use by the product/service, such as encryption, message authentication or digital signatures, use Corporate IT Department approved cryptographic algorithms and key lengths.

13.4 Wherever applicable, whether background and reference checks for both internal and outsourced vendor staff who perform security-related functions for the product/service

under review are carried out. This includes job applicants who have accepted a job offer, temporaries, consultants, full time staff as well as the outsourced vendor who is involved in product/service management and operations.

RISK ACCEPTANCE (deviation)

13.5 Does the Bank have a Risk Acceptance process wherein all the identified risks are documented and approved for any non-compliant issue that cannot be remedied and where effective compensatory controls exist?

AUTHENTICATION

13.6 Does the product/service authenticate (verifies) the identity of users (or remote systems) prior to initiating a session or transaction? Have these Authentication mechanisms been approved by then Bank's IT Department? (These include Personal Identification Numbers (PINs), passwords (static and dynamic), public keys and biometrics.)

13.7 Does the Bank verify that the initial authentication has used a mechanism that is acceptable for the application? Has the approach been approved by IT Department and required compensating controls have been implemented?

Passwords

13.8 Does the Bank have a comprehensive password construction, implementation and management policy?

Personal Identification Numbers (PINS)

13.9 Does the Bank have a policy for the Personal Identification Numbers, used by various set of customers who access the Banks systems directly using channels like ATM, Phone banking, Internet banking, Mobile banking etc?

Dynamic Passwords :

13.10 Do the Products/services using dynamic passwords for authentication, use an IT Department approved authentication server to validate the password?

Public Key Infrastructure (PKI):

13.11 Do the Products/services using Public key (or asymmetric) cryptography for authentication either on a session basis (peer authentication) or on a per-message/transaction basis (digital signatures) use approved security protocols to comply with the Public key technology standard?

13.12 For products/services that use PKI, private keys which are stored in hardware or software must be protected via an approved mechanism. The protection mechanism includes user authentication to enable access to the private key.

13.13 For products/services that use PKI, an approved process for verifying the binding of a user identity to the public key (e.g., digital certificate) is required for any server relying on public key authentication.

Biometrics Authentication:

13.14 Do the Products/Services utilizing biometrics authentication only use biometrics for local authentication?

ACCESS CONTROL

13.15 Is the access to highly privileged IDs (e.g., system administration access) strictly controlled, audited and limited in its use?

13.16 Does the product/service support the need to perform a periodic entitlement review? A periodic entitlement review process should validate access privileges.

13.17 Does the product/service support the requirement to limit individual user sessions to a maximum of X minutes of inactivity using either session time out or a password protected screen saver.

13.18 Is there a process in place to ensure that access rights reflect changes in employee or job status within X hours of the change? This includes physical access tokens and dial-in capabilities as well as any systems or applications.

13.19 Does the product/service supports the ability to disable external customer user IDs after X months of inactivity and deleted after Y months of inactivity unless they are extended through the explicit written approval of the business.

13.20 For any products/services, which has been outsourced, Is there a process in place to ensure that all platforms, services and applications are configured to meet Bank's Information Security Standards?

13.21 Does the product/service display the (A) date and time of last successful login and (B) the number of unsuccessful login attempts since the last successful login.

13.22 Does the product/service support a periodic process to ensure that all user IDs for employees, consultants, agents, or vendors are disabled after X days and deleted after Y days from the day they were not used unless explicitly approved by the business.

CRYPTOGRAPHY

13.23 Is there a cryptography/encryption policy for various types of classified information that travels/gets stored within and outside the Bank's network(s)?

NETWORK INFORMATION SECURITY

13.24 Have the Network data monitoring tools (e.g., sniffers, datascopes, and probes) utilized by the product/service been approved by the Bank's IT Department?

13.25 Is the approved Legal Affairs banner being displayed at all entry point where an internal user logs into the product/service? An automated pause or slow roll rate is in place to ensure that the banner is read. The Legal Affairs Banner usually carries the following kind of text:

"You are authorized to use this system for approved business purposes only. Use for any other purposes is prohibited. All transactional records, reports, e-mail, software and other data generated or residing upon this system are the property of the Company and may be used by the Company for any purpose. Authorized and unauthorized activities may be monitored."

NOTE: This is required for all mainframe, mid-range, workstation, personal computer, and network systems.

13.26 Has dial-in connectivity been prohibited on network-connected machine (server and workstation) except where documented and explicitly approved in writing by Business Management and the IT Department. When explicitly approved, the modem must, as a minimum control, prohibit answer or pickup until after the 5th ring.

13.27 Have the remote control products used in a dial in environment been approved by the IT Department explicitly?

13.28 Is it ensured that only software (applications / operating systems etc.) supported by the vendors only are used? (Unsupported software could be vulnerable to attacks since the vendors would not come up with the relevant patches)

13.29 Is the Anti-Virus software configured to check viruses even from the floppy drive / CD ROM drive?

E-MAIL AND VOICE MAIL RULES AND REQUIREMENTS

13.30 Is there a policy that covers e-mail & voice mail transmission of data?

13.31 Whether there are procedures, which require that all the incoming e-mail messages be scanned for virus to prevent virus infection to the Bank's network?

13.32 Whether all e-mails are identified with a user's name or e-mail ID to facilitate tracking? Whether e-mail ID allotted to a user is prevented from being used by another user?

13.33 Ensure that users do not forward the e-mail messages automatically without prior approval.

13.34 Whether there are procedures to ensure that users do not send confidential or sensitive information via e-mail? Whether the information transmitted through e-mail is encrypted?

13.35 Whether all e-mails sent and received by employees via Bank's network are treated as Bank's records? Is there procedure to monitor them?

INFORMATION SECURITY ADMINISTRATION

13.36 Is there an approved document clearly outlining the Information Security Administrator's (ISA) responsibility?

13.37 Are all the administrative actions (e.g., adding/deleting users, changes to entitlements/passwords) backed up by an independent review?

13.38 Does the ISA function review all security audit logs, incident reports, and on-line reports at least once per business day?

13.39 In case of Wide Area Networks (WAN), are the router tables maintained securely in Routers?

13.40 Are router login IDs and passwords treated as sensitive information and managed by authorised administrators?

13.41 Are all changes to router table entries logged and reviewed independently? Are access violations taken note of, escalated to higher authority and acted upon in a timely manner?

13.42 Is there a process to report all unusual or suspicious activity? (Reporting to IT Department, investigating immediately, and bringing the case to closure without delay)?

13.43 Does the ISA function assess compliance with their security procedures quarterly and reports their results to the IT Department?

13.44 Have all the all security related administrative procedures under the control of the ISA been documented and approved by management (annual exercise)? At minimum procedures should include:

Information Ownership

Data Classification

User registration/Maintenance

Audit Trail review

Violation logging and reporting

Sensitive activity reporting

Semi-Annual Entitlement Reviews

Password resets

Escalation reporting

MICROCOMPUTER/PC SECURITY

13.45 Does the LAN servers, mail servers, and microcomputers have IT Department approved anti-virus products installed?

13.46 Are all product/service specific microcomputers/PCs secured against removal and theft commensurate with the value of the computer and information it holds along with a process to report any thefts to the IT Department?

13.47 Are microcomputers / PCs having sensitive information protected with power on password to prevent unauthorised access?

13.48 Are sensitive data in such microcomputers / PCs backed up and preserved properly with records to ensure recovery in case of failure?

AUDIT TRAILS

13.49 Does the audit trail associate with the product/service support the ability to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, highly privileged accounts and emergency IDs?

13.50 Does the financial transactions as well as additions, changes and deletions to customer's demographic data/important statistics, get recorded in the product/service audit trail?

13.51 Does the audit trail for product/service record all identification and authentication processes? Also Is there a retention period for the Audit trails

13.52 Does the audit trail associate with the product/service log all actions by the ISA?

13.53 Is there a process to log and review all actions performed by systems operators, systems managers, system engineers, system administrators, security administrators, and highly privileged IDs.

13.54 Is there a process in place to log and review actions performed by emergency IDs associated with the product/service?

VIOLATION LOGGING MANAGEMENT

13.55 Whether the product/service is capable of logging the minimum criteria specified to log and report specific security incidents and all attempted violations of system integrity

13.56 Are the product/service owners aware of their responsibilities with respect to Security incident reporting?

INFORMATION STORAGE AND RETRIEVAL

13.57 Has all the media (File/Floppy/Disks etc) under the control of the product/service owner been marked with the classification and securely stored with access restricted to authorized personnel only?

13.58 Is there a process in place to ensure that all media under the control of the product/service owner containing critical information is destroyed in a manner that renders it unusable and unrecoverable?

13.59 Is there a procedure in place that enforces and maintains a clean desk program, which secures all critical information from unauthorized access?

PENETRATION TESTING

13.60 Is it ensured that products/services that use the Internet for connectivity or communications have undergone a successful penetration test prior to production implementation?

13.61 Is there a penetration test process that ensures whether modifications to the product/service that uses the Internet for connectivity or communication have been reviewed to determine whether a subsequent penetration test is warranted?

13.62 Is there an intrusion detection system in place for all the external IP connections?

14. Maintenance

Maintenance will include the following: -

1. Change Request Management and version control
   1.1. Software developed in-house
   1.2. Software purchased from outside vendor
2. Software trouble shooting
3. Backup and recovery
4. Hardware maintenance
5. Training

Wherever Application Service Provider, who owns the Hardware and maintains the OS/ application software, processes the data for the User, detailed Service Level Agreement should cover entire maintenance.

Change Request Management and Version Control

Software developed in-house

14.1 Check whether requests for changes are initiated by users in a structured change request form (CRF) with pre-printed numbers.

14.2 Are these change requests inwarded in a manual / electronic register with CRF number before initiating the change.

14.3 Are the change requests subjected to feasibility study?

14.4 Verify whether the change request is approved by the Management before effecting the changes in the software and the same is recorded on the CRF.

14.5 Verify whether the changes are made only in the test environment and not in the live environment (separation of test and production libraries).

14.6 After making changes, are they tested adequately before implementation (unit testing, integrated testing, regression testing, etc.)? All these testing procedures should happen only in the test library.

14.7 Once the programs are ready after testing, are they approved by a senior programmer / Departmental Head? Are such approvals recorded on the CRF?

14.8 After approving the changes, are the changed programs transferred to production library by an independent person who does not have programming / development responsibilities?

14.9 Does the production library have both sources and executables of the latest version of the programs?

14.10 Check whether the programmers are not given access in the production library. Similarly, check whether the access to the test library is restricted to programmers only.

14.11 Verify if the changes are updated in the user, technical, operations and all other relevant manuals to reflect the current state of the software. Is the CRF updated to this effect?

14.12 Verify if implementation guidelines are prepared by the programmers for properly implementing the changes in the user sites. Are they approved?

14.13 Verify if the changes are implemented at the Users' sites in accordance with the implementation guidelines. Is the CRF updated to this effect?

14.14 After completing all these steps, is the open entry in the change request register rounded off for the relevant CRF number, to bring it to a logical conclusion?

14.15 Is the completed CRF filed along with the system documents?

14.16 Are there procedures to review and monitor all the pending change requests and initiate timely action to resolve the same.

Version Control

14.17 Verify the procedure of roll out of software to the Users sites. Check who is creating the executables from the changed source code for implementation in the user sites? Ensure that that such person(s) is / are independent of development activities.

14.18 Verify if the access to the compilers is restricted to only authorised persons who are empowered to create the executables from the source code.

14.19 Check whether identity of different programs is maintained between any two software release and each release contains all the changes to different programs from the previous release.

14.20 Check whether each release is given a version number.

14.21 Verify if proper records are maintained to reflect the different version numbers of the software, their composition and location. The latest version should be easily differentiated when compared with the older versions.

14.22 If possible, take the latest version of any one program in the test library and arrange to compile the same to arrive at the new exe file. Note down the byte size of the new 'exe' file and compare whether the byte size of the exe program in the live area in the user site is the same as the size noted.

14.23 If multiple User sites are there, verify the control mechanism to ensure whether the same software is being implemented in all such user sites.

14.24 If there are exceptions to certain Users, verify if those exception modules of the software are kept in the central control library from where the software is rolled out.

14.25 Verify if there are any register/database containing the information about which site has which version.

14.26 Check and ensure if backup of all versions of the software are held both onsite and off-site in fire resistant cabinets with proper records.

Software procured from outside vendor

14.27 Verify if there is Annual Maintenance Contract for software and check whether it is currently in force.

14.28 Check if requests for changes are initiated by users in a structured change request form (CRF) with pre-printed numbers.

14.29 Verify if the change request is approved by Management before asking the vendor to effect the changes in the software.

14.30 Are these change requests (CRFs) inwarded in a manual / electronic register before sending it to the vendor for their making changes.

14.31 For all the changes effected and implemented by the vendor, check whether release notes have been provided for all such patches / releases. If so, does the release notes given by the vendor contain the CRF number submitted by the Bank.

14.32 Check whether the release notes have been circulated to all the users.

14.33 Check whether the open entry in the inward register having the CRF number attended by the vendor is rounded off to reflect the latest pending position.

14.34 Check whether the vendor has updated the user's and operations' manuals to reflect the current state of the software and delivered the same to the Bank.

14.35 Check the procedure for marking off the entries in the inward register for CRFs maintained at CPPD/ IT and ensure whether the current list of outstanding requests are complete and accurate.

14.36 Is there procedure to review and monitor all the pending change requests and initiate timely action to get the same resolved by the vendor in a time-bound manner.

14.37 Verify Service Level Agreement (SLA) with the vendor. Does it lay down the basis of billing, say, based on 'x' number of lines of coding or based on 'y' man hours of effort, etc. Check whether the billing made by the vendor is in accordance with the SLA. Test check whether the billing raised is accurate.

14.38 Does the SLA have penalty clause for delay on the part of the vendor to deliver the changes after submitting the CRF? If so, for any delays on the part of the vendor, does the Bank invoke the penalty clause and charge penalty?

14.39 Verify if any escrow arrangement exists for the source code. If so, check who is the escrow party and inspect their site and check whether a copy of the latest version of the source code is stored there in proper condition with records.

14.40 Check whether one copy of full set of the latest documentation of the software is also kept with the source code in the Escrow's location.

14.41 Check and ensure that Escrow party cannot have unilateral access to the source code and documentation without the knowledge of the software vendor and the Bank.

14.42 Check and ensure if backup of the latest version of the software provided by the vendor is held both onsite and off-site in fire resistant cabinets with proper records.

Software Trouble Shooting

Help Desk

14.43 Check if user calls are logged in a register (manual or electronic) in the Help Desk with a unique identification number for each call. Preferably, the numbering should be serial and unique for each user site.

14.44 Is this number recorded in a Help Desk register in the user's site with nature of the call, date and time of call?

14.45 Does the Help Desk register in the user site reflect all the call identification numbers serially without any missing number in between?

14.46 Is the date and time of resolving the trouble recorded in the Help Desk register? Does it correspond and tally with the records maintained at the Help Desk?

14.47 Are the calls attended to in a timely manner?

14.48 Does Help Desk issue call sheet with solution given duly signed by the user?

14.49 If the trouble shooting is attempted by the Help Desk personnel remotely, check whether any sensitive password was divulged by the user to the Help Desk. This should have been recorded in the Help Desk register both at user site and at Help Desk.

14.50 If sensitive password is revealed to the Help Desk, check the system and application logs and ensure whether the changes made are appropriate to the trouble reported by the user.

14.51 Check whether command log is printed and submitted to the user site, duly signed by the Help Desk official and authenticated by the Help Desk in-charge.

File / Data reorganisation

14.52 If the software works on a RDBMS, check whether file / database reorganisation is carried out at the user site timely to avoid any processing error.

14.53 If any addition to datafile / tablespace is made, are they approved and in accordance with the software implementation guidelines.

14.54 If operating system / database fine tuning is carried out, are they documented in the error log / Help Desk register.

14.55 As most of these activities require sensitive passwords, does the usage of the same recorded in the password usage register duly signed by the support personnel and user.

14.56 Verify the command logs and ensure that the command and command results are appropriate to file / database reorganisation / fine tuning, etc.

14.57 Verify if due to O/S upgrades any constraint is there in the application software.

14.58 Verify if the interface software is properly tested and implemented if the User is using 2 or 3applications and data is transmitted through this interface application

Backup and recovery

Software

14.59 Verify if a latest copy of backup of software (Operating System, RDBMS, application, etc.) is taken and preserved at the user site.

Data

14.60 Verify if different types of data backup are taken periodically at specified intervals as advised by the software developer / vendor.

14.61 Are there proper records for noting the media in which different data backups are stored, data type, location where it is stored, date of backup, due date for recycle, etc.

14.62 Is one copy of data backup kept in an offsite location with proper records?

14.63 Does the database / system administrator at the user site carry out restoration testing of these backups periodically? Is it recorded and authenticated?

14.64 Are users involved in such restoration testing ?

Purging of data

14.65 Verify if there is an archival policy and data housekeeping is as per this policy.

14.66 Verify if this archival data can be read as and when required

14.67 Verify if these archival data is stored in safe place.

14.68 Verify if archived data is deleted from the current running system.

14.69 Verify if the printed reports are deleted from the system.

Hardware maintenance

14.70 Verify if there is any Service Level Agreement between the hardware vendor and CPPD / IT Department.

14.71 Check and ensure that the AMC with the vendor for maintenance of hardware equipments is active and currently in force.

14.72 Verify if the network diagram is available at the user site.

14.73 Does the user site have the names and photographs of the service personnel and are they identified by the users before allowing them to handle the hardware.

14.74 Verify if the hardware inventory is maintained at the user site. Ensure whether the physical stock of hardware items matches with the hardware inventory.

14.75 Verify if the hardware maintenance register is maintained, with full details such as nature of trouble, date and time of reporting, name of the vendor, Engineer's name, date and time of resolution, signature of DBA, signature of Engineer, Initials of Head of the user site.

14.76 Verify if there is a databank of malfunctions of hardware. If so, examine whether similar types of hardware errors are recurring. Check the steps taken by the users / CPPD / IT to arrest this trend.

14.77 In case hardware are taken by the vendors for servicing / repair, does the user site ensure that the equipment does not contain sensitive live data.

Training

14.78 Verify if the Users are given adequate training on the application systems functionalities

14.79 Verify if the Technical persons are given adequate training in the technical details of the application system, to provide necessary trouble shooting / help to users.

14.80 Verify if the Users are aware of the steps to be carried in case of contingency due to non-availability of systems.

15. Internet Banking

Information Systems Security Framework

15.1 Is there a security policy duly approved by the Board of Directors? Is there segregation of duty of Security Officer/Group dealing exclusively with information systems security and Information Technology Division which actually implements the computer systems? Is the role of an Information Security Officer independent in nature?

15.2 Is the role of an information system auditor independent in nature? (It should be independent of Operations and Technology Unit)

15.3 Bank should ensure that Information Systems Auditor forms part of their Internal Audit Team.

15.4 Bank should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches. Bank should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate their security personnel and also the end-users on a continuous basis.

15.5 Bank should subscribe for the Systems Alerts/Patches. Information Systems Auditor should ensure that all vulnerable patches are applied on a periodic to prevent outsiders exploiting the Bank’s systems.

15.6 Under the present legal requirements there is an obligation on Banks to maintain secrecy and confidentiality of customer’s accounts. In the Internet banking scenario, the risk of Banks not meeting the above obligation is high on account of several factors. Despite all reasonable precautions, banks may be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking/ other technological failures. Does the bank, therefore, institute adequate risk control measures to manage such risks?

15.7 In order to address the risk of liability to customers on account of breach of secrecy, denial of service etc., does the Bank follow a privacy policy?

15.8 Some of the indicated areas which all Banks need to include as part of the Privacy Policy is given below

- Banks should safeguard, according to strict standards of security and confidentiality, any information customers share with them.
- Banks will not reveal customer information to any external organization unless they have previously informed the customer in disclosures or agreements, have been authorized by the customer, or are required by law or our regulators.
- Whenever Banks hire other organizations to provide support services, they should require them to conform to our privacy standards and to allow us to audit them for compliance.

Web Server

15.9 Is the web server configured to be a stand-alone unit without any membership to any domain inside the Bank's IT architecture?

15.10 Ensure whether the web server is ported with latest versions of patches and service packs. Specifically, the OS vendor releases patches and service packs with appropriate fixes to prevent Denial of Service attack. These should have been applied to prevent such attacks on the web server.

15.11 All security settings applicable to the operating system in which the web server operates should have been implemented as per IT security policy. Check and ensure this.

15.12 With regard to Super User account :-

- Check whether the super user account in the web server is enabled for login only on the system console and not from across the network. Perhaps this is applicable to all user accounts in the web server.

- Check if appropriate parameters are implemented in the operating system of the web server so that the super user account will lock out if too many unsuccessful attempts are made across the network, but remain unlocked at the system console.

15.13 Check if sensitive operating system related executable program files and data files on the web server are not stored on public area but in any other secure location with audit duly enabled.

15.14 IP routing should be disabled in the web server. Check and confirm this.

15.15 Ensure that unauthorized ports for e.g., UDP port No.443 are not allowed inside the web server. Also, ensure that unnecessary services like ftp, messenger, SMTP, telnet, etc. are not installed and active on the web server.

15.16 The facility to shutdown the machine should be restricted to the system console on the web server. Check and ensure this.

15.17 Access to floppy drive, CD-ROM drive, etc. should be restricted in the web server to interactive only to prevent these devices from being shared by all processes on the system. Check and ensure this.

Logs of activity

15.18 Ensure that auditing is enabled in the web server's operating system and whether the logs are reviewed and authenticated by authorized officials periodically.

15.19 Check if audit trail is enabled on the firewall to log the changes made to the rule base settings and verify whether the logged entries are approved by higher authorities in the IT Department.

15.20 Whether the system administrators are monitoring the logs produced by the Intruder Detection System (IDS) (An intrusion detection system helps in recognizing Security threats and is capable of scanning packets for vulnerabilities. It ensures that distributed denial of service attacks are prevented) and escalating the access violations to the

attention of senior management in IT department for guidance. Are these documented and appropriate corrective actions taken?

15.21 Check whether audit trails are enabled for administration activities and whether entries logged in the audit trail are in accordance with process flow chart and no unauthorized activity has been carried out.

De-militarized zone and Firewall

15.22 Are all Internet connections are routed through a Firewall? Does a dedicated team manage the Firewall? Are the ports opened only on a "need to have" basis?

15.23 Is there an Intruder Detection System (IDS) implemented?

15.24 Are the application and database servers kept separated from the web server in the de-militarized zone?

15.25 Is the de-militarized zone separated from the Internet cloud by means of a Firewall? (Firewall procurement should be through an approval mechanism, which ensures that only firewalls of highest standards are procured).

15.26 If the de-militarized zone is connected to the Intranet within the Bank, it should be separated by a Firewall. Check and ensure the same.

15.27 Check whether the Firewall rule base is treated as a sensitive information and knowledge of the same is restricted to only authorized officials in the IT / Computer operations department.

15.28 Ensure that the decision to open specific firewall ports/rule base is approved in accordance with IT Security Policy (IT Security Policy should list out such ports) e.g. firewalls should block unwanted ports running services such as ftp, telnet, SMTP, etc. into the de-militarized zone. Ideally, only http and https ports are allowable. Check and verify this.

Security Review of all Servers used for Internet Banking

15.29 Carry out a Operating System Security review on all the servers used for internet banking apart from web server as stated in (I) above and ensure that all security parameters have been properly set as per Security Policy.

Database and System Administration

15.30 Has the Bank designated a Database Administrator with clearly defined roles?

15.31 Has the Bank designated System Administrator(s) with clearly defined roles?

15.32 Check whether process flow of administration activities is documented and approved by the Head of Operations and whether the administrators are conversant with the process flow.

15.33 Carry out an application control review of the administration module and ensure whether the functionality as described in the process flow document are adequately met by the module.

15.34 Examine who has access to the Super User account in the administration module? Examine the procedures for custody and usage of this password and records maintained for the same. Are all usages recorded by the administrator authenticated by appropriate authority.

15.35 Obtain a list of all administrator accounts in the administrator's module and check whether all are attributable to personnel doing the administration job. Extraneous admin IDs should be identified and reported for deletion.

15.36 Check whether the menu options in the admin module are assigned to different administrators on need to know basis, based on functionality offered by the menu options and the work allotment made to the administrator.

15.37 Obtain the list of menu options in the Internet banking module for customers and whether such menu options are assigned to user (customer) IDs only as per their request and as per the policy of the Bank.

15.38 Pay particular attention to user (customer) IDs, which are provided with third party funds transfer facility on the Internet and verify whether they are backed by proper customer request in writing.

15.39 Does the Bank have proper infrastructure and schedules for backing up data? Is the backed-up data periodically tested to ensure recovery without loss of transactions in a time frame as given out in the bank's security policy? Is Business Continuity ensured by setting up disaster recovery sites? Are these facilities tested periodically?

15.40 Check the procedure for creation of different user accounts for the customers for usage on the internet and whether they are backed by valid customer request for such facility.

Operational Activities

15.41 Considering the legal position prevalent, is it ensured that the Banks not only to establish the identity but also to make enquiry about integrity and reputation of the prospective customer? Therefore, is it ensured that even though request for opening account can be accepted over Internet, accounts are opened only after proper introduction and physical verification of the identity of the customer? Is there a Legal Contract with the customer in place covering the risks of communicating using the Public Network?

15.42 Pay particular attention to customers whose constitution is other than "individual", particularly corporate accounts and check whether appropriate account opening documentation have been submitted by such customers for internet banking.

15.43 Check if any customer is provided with multiple user IDs, if he/she is not a joint account holder, but only single.

15.44 Any account linkage activity should take place only after ensuring that the user accounts are created based on valid customer requests.

15.45 Check if user-IDs are linked to multiple bank accounts. If so, verify whether such accounts pertain to the same customer only.

15.46 Check the procedure for enabling the customer user ID on the internet and verify whether adequate precautions are taken by the operations personnel to identify the customer before enabling. Account enablement process should be decided and signed off before product launch. Entire process should be auditable and audit trails should be enabled for the same (Each Bank can decide whether they can pre-enable or post-enable the user accounts based on their policy).

15.47 Check the procedure for creation of new password for customers who report having forgotten the password. Verify the procedure for ensuring the identity of the customer before creating the new password.

15.48 Verify whether adequate records (either electronic or manual) are maintained for the customer user IDs created, enabled, new passwords provided, etc. and whether they are authentic. Test check the instances of change of customer's passwords and whether they are backed by valid customer requests.

15.49 Do all applications of banks have proper record keeping facilities for legal purposes? It may be necessary to keep all received and sent messages both encrypted

Application Control Review of Internet Banking Application

15.50 Does the software allow creation of user-IDs in the same name more than once?

15.51 Does the software encrypt the passwords one way and store the same in encrypted form in the database?

15.52 Does the software display the password as it is keyed in? (It should not be displayed on the screen).

15.53 Does the software lock the user-id if it is used for X unsuccessful times to logon to the system?

15.54 Does the software force the User to change the password at set periodical intervals?

15.55 Does the software maintain password history i.e., the same password should not be used again on rotation basis.

15.56 Check whether the software logs the instances of change of user's (customer's) password in the audit trail?

15.57 Does the software allow automatic logical deletion of inactive user IDs after certain period of time?

15.58 Does the system maintain password length to be of minimum 6 or 8 characters or as the case may be with combinations of alpha, numeric and special characters?

15.59 Check whether the menu options available on the web page for a customer after logging on to the system provide only appropriate functionality as designed and no deviation is possible.

Application Security

15.60 Is the Security infrastructure properly tested before using the systems and applications for normal operations? Following needs to be taken care of for ensuring that Security infrastructure is tested properly before using the systems and applications:

- As part of the System Development Life Cycle (SDLC), during the development stage an Information Security Review needs to be conducted covering the entire system and architecture review
- Comprehensive Information Security related checks needs to be conducted during the Coding & Testing stage
- On completion of User Acceptance testing (UAT), all Internet related systems or applications needs to be penetration tested by an independent party.

- Banks should enter into an Agreement with the independent party who conducts the penetration testing covering both Legal and Contractual terms.

15.61 Following should be covered as part of penetration tests / vulnerability tests: -

1. Check for following common vulnerabilities :
   - IP Spoofing
   - Buffer overflows
   - Session hijacks
   - Account spoofing
   - Frame spoofing
   - D-DoS attacks
   - Caching of web pages
   - Cross-site scripting
   - Cookie handling
2. As per RBI's guidelines PKI (Public Key Infrastructure) is the most favoured technology for secure Internet banking services. Since Government & RBI is in the process of identifying a PKI service provider, it may take some time to implement PKI in all the Banks. However, as it is not yet commonly available, does the bank use the following alternative system during the transition, until the PKI is put in place:
   - A static ID and password login process.
   - Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the Banks themselves using a Certificate Server.
   - The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

----@------