1.Asset Management

Prior to procuring any new ICT assets, compatibility assessment (with existing  
system) shall be performed by the Bank or NBFI.

All ICT asset procurement shall be complied with the procurement policy of Bank  
or NBF

Each ICT asset shall be assigned to a custodian (an individual or entity) who will  
be responsible for the development, maintenance, usage, security and integrity  
of that asset

All ICT assets shall be clearly identified and labeled. Labeling shall reflect the  
established classification of assets

Bank or NBFI shall maintain an ICT asset inventory stating significant details (e.g.  
owner, custodian, purchase date, location, license number, configuration, etc.)

Bank or NBFI shall comply with the terms of all software licenses and shall not  
use any software that has not been legally purchased or otherwise legitimately  
obtained

Outsourced software used in production environment shall be subjected to  
support agreement with the vendor

Bank or NBFI shall approve list of Software which will only be used in any  
computer.

2.Desktop/Laptop Devices Controls

Desktop computers shall be connected to UPS to prevent damage of data and  
hardware

Desktop computers, laptops, monitors, etc. shall be turned off at the end of each  
workday

Laptops, computer media and any other forms of removable storage containing  
sensitive information (e.g. CD ROMs, Zip disks, PDAs, Flash drives, external harddrives) shall be stored in a secured location or locked cabinet when not in use.

Access to USB port for Desktop/Laptop computers shall be controlled

User identification (ID) and authentication (password) shall be required to access  
all desktops and laptops whenever turned on or restarted.

3.Server security control

* Users shall have specific authorization for accessing servers with defined set of  
  privileges
* Inactive session shall be expired after a defined period of inactivity
* Bank or NBFI shall ensure the security of file sharing process. File and print shares  
  must be disabled if not required or kept at a minimum where possible
* All unnecessary programs shall be uninstalled from production servers.

**4. Data centre control**

**Physical security**

* Various types of physical locks, including conventional key locks, electronic access badge locks, cipher locks, combination locks, and biometric locks
* Security guards
* Video surveillance cameras
* Heating, ventilation, and cooling (HVAC) systems
* Insurance coverage over hardware and the costs to re-create data
* Procedures to perform periodic backups of system software, application programs, and data as well as storage and rotation of the backup media to a secure off-site location

**Logical security**

**User access**

* The Bank or NBFI shall closely monitor non-employees (contractual, outsourced,  
  or vendor staff) for access restrictions.
* Each user must have a unique User ID and a valid password.
* User ID Maintenance form with access privileges shall be duly approved by the  
  appropriate authority.
* User access shall be locked for unsuccessful login attempts.  
  User access privileges must be kept updated for job status changes.
* The Bank or NBFI shall ensure that records of user access are uniquely identified  
  and logged for audit and review purposes.

**Password**

* Password controls shall include a change of password upon first logon.
* Password definition parameters shall ensure that minimum password length is  
  maintained according to Bank's Policy (at least 6 characters)
* Password shall be combination of at least three of stated criteria like uppercase,  
  lowercase, special characters and numbers
* Maximum validity period of password shall not be beyond the number of days  
  permitted in the Bank's Policy
* Parameter to control maximum number of invalid logon attempts shall be  
  specified properly in the system according to the Bank’s Policy (maximum 3  
  consecutive times).

**5. Environmental Security**

* No eating/ drinking sign
* Uninterrupted Power Supply (UPS) with backup units  
  b) Backup Power Supply  
  c) Temperature and humidity measuring devices  
  d) Water leakage precautions and water drainage system from Air Conditioner
* CCTV

**6. Internet access management**

* Internet access shall be provided to employees according to the approved  
  Internet Access Management Policy
* Access to the Internet from bank premises and systems must be routed through  
  secure gateways
* Employees shall be prohibited from establishing their own connection to the  
  Internet using banks’ systems or premises.

**7. Email management**

* Email system shall be used according to the Bank’s or NBFI's policy.
* Access to email system shall only be obtained through official request
* Email shall not be used to communicate confidential information to external  
  parties unless encrypted using approved encryption facilities.
* Bank email system is principally provided for business purposes. Personal use of  
  the bank email system is only allowed under management discretion and  
  requires proper permission; such personal use may be withdrawn or restricted at  
  any time.
* Corporate email address must not be used for any social networking, blogs,  
  groups, forums, etc. unless having management approval

**8. Vendor Selection**

There must be a core team comprising of personnel from Functional  
Departments, ICT Department and Internal Control and Compliance Department  
for vendor selection.

Vendor selection criteria for application must address followings:  
a) Market presence  
b) Years in operation  
c) Technology alliances  
d) Extent of customization and work around solutions  
e) Financial strength  
f) Performance and Scalability  
g) Number of installations  
h) Existing customer reference  
i) Support arrangement  
j) Local support arrangement for foreign vendors  
k) Weight of financial and technical proposal

Service contracts with all service providers including third-party vendors shall  
include:  
a) Pricing  
b) Measurable service/deliverables  
c) Timing/schedules  
d) Confidentiality clause  
e) Contact person names (on daily operations and relationship levels)  
f) Roles and responsibilities of contracting parties including an escalation  
matrix  
g) Renewal period  
h) Modification clause  
i) Frequency of service reporting  
j) Termination clause  
k) Penalty clause  
l) Warranties, including service suppliers’ employee liabilities, 3rd party  
liabilities and the related remedies  
m) Geographical locations covered  
n) Ownership of hardware and software  
o) Documentation (e.g. logs of changes, records of reviewing event logs)  
p) Right to have information system audit conducted (internal or external).

**9. In-house Software Development**

Detailed business requirements shall be documented and approved by the  
competent authority.

Detailed technical requirements and design shall be prepared.  
Application security and availability requirements shall be addressed.  
Developed functionality in the application shall be in accordance with design  
specification and documentation.  
Software Development Life Cycle (SDLC) with User Acceptance Test (UAT) shall  
be followed and conducted in the development and implementation stage.  
User Verification Test (UVT) for post deployment shall be carried out.  
System documentation and User Manual shall be prepared and handed over to  
the concerned department.  
Source code must be available with the concerned department and kept secured.  
Source code shall contain title area with author name, date of creation, last date  
of modification and other relevant information.  
Application shall be in compliance with relevant controls of Bank’s ICT Security  
Policy.

**10. Software Documentation**

Documentation of the software shall be available and safely stored.  
Document shall contain the followings:  
a) Functionality  
b) Security features  
c) Interface requirements with other systems  
d) System Documentation  
e) Installation Manual  
f) User Manual  
g) Emergency Administrative procedure