उत्तराखण्ड राज्य सहकारी बैंक लि०
Uttarakhand State Co-Operative Bank Ltd.

INFORMATION SYSTEMS SECURITY & AUDIT POLICY

प्रस्ताव संख्या – 12
दिनांक – 03/06/2023

Uttarakhand State Co-Operative Bank Limited

Policy/Guidelines on

INFORMATION SYSTEMS SECURITY & AUDIT POLICY

DOCUMENT CONTROL

Document Title	Policy/Guidelines on Information Systems Security & Audit Policy
Document Code	
Document Version	
Approved By	
Approved On	
Effective Date	
Last Review Date	

PREAMBLE:

The Information Systems (I S) Security & Audit Policy approved by the Board on _____ is in place and being implemented effectively. I S Security & Audit policy will be subjected to an annual review to ensure its continued relevance and effectiveness.

Basis for Information Systems (IS) Security & Audit Policy:

The framework and Policy formulation for audit of technological risks has emanated from the report of working group constituted by RBI for finalizing the standards and procedures for IS audit and IS security for the banking and financial sector, titled "Information Systems Audit Policy" including Information Systems Security guidelines and latest RBI working group guidelines on electronic banking and Information security published in April 2011.

IT Security Policy

Information Security

Information Security Policies are the cornerstone of information security effectiveness.

The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide human behaviour in an attempt to reduce the risk to information assets by accidental or deliberate actions.

Confidentiality: Protecting information from unauthorized disclosure like to the press, or through improper disposal techniques, or those who are not entitled to have the same.

Integrity: Protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.

Availability: Ensuring information is available when it is required. Data can be held in many different areas, some of these are:

- Network Servers
- Personal Computers and Workstations
- Laptop and Handheld PCs
- Removable Storage Media (Floppy Disks, CD-ROMS, Zip Disks, Flash Drive etc.)
- Data Backup Media

Data Loss Prevention

Leading Causes of Data Loss:

- Natural Disasters
- Viruses
- Human Errors
- Software Malfunction
- Hardware & System Malfunction

Computers are more relied upon now than ever, or more to the point the data that is contained on them. In nearly every instant the system itself can be easily repaired or replaced, but the data once lost may not be retraceable. That's why of regular system backups and the implementation of some preventative measures are always stressed upon.

Natural Disasters

While the least likely cause of data loss, a natural disaster can have a devastating effect on the physical drive. In instances of severe housing damage, such as scored platters from fire, water emulsion due to flood, or broken or crushed platters, the drive may become unrecoverable.

The best way to prevent data loss from a natural disaster is an offsite back up.

Since it is nearly impossible to predict the arrival of such an event, there should be more than one copy of the system back up kept, one onsite and one off. The type of media back up will depend on system, software, and the required frequency needed to back up. Also be sure to check backups to be certain that they have properly backed up.

Human Errors

Even in today's era of highly trained, certified, and computer literate staffing there is always room for the timelessness of accidents. There are few things that might be followed: -

- Be aware. It sounds simple enough to say, but not so easy to perform. When transferring data, be sure it is going to the destination. If asked "Would you like to replace the existing file" make sure, before clicking "yes".
- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Take extra care when using any software that may manipulate drives data storage, such as: partition mergers, format changes, or even disk checkers.
- Before upgrading to a new Operating System, take back up of most important files or directories in case there is a problem during the installation. Keep in mind slaved data drive can also be formatted as well.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.

Software Malfunction

Software malfunction is a necessary evil when using a computer. Even the world's top programs cannot anticipate every error that may occur on any given program. There are still few things that can lessen the risks:

- Be sure the software used will meant ONLY for its intended purpose. Misusing a program may cause it to malfunction.
- Using pirated copies of a program may cause the software to malfunction, resulting in a corruption of data files.
- Be sure that the proper amount of memory installed while running multiple programs
- simultaneously. If a program shuts down or hangs up, data might be lost or corrupt.
- Back up is a tedious task, but it is very useful if the software gets corrupted.

Hardware Malfunction

The most common cause of data loss, hardware malfunction or hard drive failure, is another necessary evil inherent to computing. There is usually no warning that hard drive will fail, but some steps can be taken to minimize the need for data recovery from a hard drive failure:

- Do not stack drives on top of each other-leave space for ventilation. An over heated drive is likely to fail. Be sure to keep the computer away from heat sources and make sure it is well ventilated.
- Use an UPS (Uninterrupted Power Supply) to lessen malfunction caused by power surges.
- NEVER open the casing on a hard drive. Even the smallest grain of dust settling on the platters in the interior of the drive can cause it to fail.

- If system runs the scan disk on every reboot, it shows that system is carrying high risk for future data loss. Back it up while it is still running.
- If system makes any irregular noises such as clicking or ticking coming from the drive. Shut the system down and call Hardware Engineer for more information.

Protection of computer from virus infection

- Make regular backups of important data.
- Install antivirus software on computer and use it daily.
- Update the antivirus software with the latest signature files on weekly/forthnightly basis. Antivirus software does no good unless it is frequently updated to protect against the most recent viruses.
- Upgrade the antivirus software when new releases are provided.
- Never open or execute a file or e-mail attachment from an unidentified source. If user is unsure of the source, delete it. Recent viruses have been written so that they come from friends and colleagues. Be cautious with attachments even from trusted sources. If it was sent knowingly, an attachment could still contain a virus. Saving it as a file and running the virus scan software will catch any virus that it has been set up to find, therefore will catch most of them.

Using Floppies / CD / Flash Drives

- CDs or Flash Drives should be used in consultation with system administrator/incharge computer center and should be scanned before use.
- Unofficial CDs or Flash Drives should not be used on office systems.
- CDs or Flash Drives should be write-protected if data is to be transferred from floppy to system.

Password

- Keep the system screen saver enabled with password protection.
- Don.t share or disclose your password.
- User should not have easily detectable passwords for Network access, screen saver etc.
- A strong password must be as long as possible, include mixed-case letters, include digits and punctuation marks, not be based on any personal information, not be based on any dictionary word, in any language.
- Never use the same password twice.
- Change password at regular intervals

Physical Safety of System

- Protect the system from unauthorized use, loss or damage, e.g. the door should be locked when not in the office.
- Keep portable equipment secure.
- Position monitor and printers so that others cannot see sensitive data.
- Keep floppy disks and other media in a secure place.
- Seek advice on disposal of equipment.
- Report any loss of data or accessories to the System Administrator/ incharge computer center.
- Keep the system and sensitive data secure from outsiders.
- Get authorization before taking equipment off-site.
- Take care when moving equipment (Read instruction on moving equipment).
- Install UPS system with adequate battery backups to avoid any data loss or corruption due to power failure.
- System should be properly shut down before leaving the office.
- Log-off the system if you are leaving your seat.
- Never remove the cables when your PC is powered ON since this can cause an electrical short circuit.

- Do not stop scandisk if system prompts to run it at the time of system startup. □ Always use mouse on mouse pad.
- Be gentle while handling keyboard and mouse.
- Do not open case of the hardware.
- Make sure that there is some slack in the cables attached to your system.

General Instructions

- In case of uncertainty about a task, make sure there is a copy of the data to restore from.
- Follow instructions or procedures that comes from System administrator/Incharge computer centre time to time.
- Users are not supposed to do his or her personal work on computers.
- Please intimate System administrator/Incharge computer centre in case of system malfunction.
- User should always work on his/her allotted machines. In case of any urgency/emergency user may use other's machine with consultation of System administrator/In charge computer centre.
- Antivirus software should be updated timely in consultation with System Administrator/In charge computer centre.
- Don't give others the opportunity to look over your shoulder if you are working on sensitive data/contents.
- Do not use unnecessary shareware.
- Do not install or copy software on system without permission of System administrator/In charge computer centre.
- Avoid unnecessary connectivity of Internet.
- Don't panic in case system hangs. Report it your IT Nodal Officer/System Administrator/In charge computer centre.
- If lock and key system is available then user should ensure the security of all the parts of the computer.
- Please ensure that preinstalled Antivirus is running on the system.
- Food and drinks should not be placed near systems. Cup of Tea/ Coffee or water glass should not be on CPU or Monitor or Key Board.
- Always power off the system when cleaning it.
- Never use wet cloth for wiping the screen.
- Never shut the system down while programs are running. The open files will, more likely, become truncated and non-functional.
- Never stack books/ files or other materials on the CPU.

Information Systems Audit (IS) Policy: -

Preamble: -

In the past decade, with the increased technology adoption by Banks, the complexities within the IT environment have given rise to considerable technology related risks requiring effective management.

This led to implement an internal Control framework, based on various standards and its own control requirements and the current RBI guidelines. As a result, Bank's management and RBI, need an assurance on the effectiveness of internal controls implemented and expect the IS Audit to provide an independent and objective view of the extent to which the risks are managed.

As a consequence, the nature of the Internal Audit Department has undergone a major transformation and IS Audits are gaining importance as key processes are automated, or enabled by technology. Hence there is a need for banks to re assess the IS Audit processes and ensure that IS Audit objectives are effectively met.

Objectives

It is essential for the Bank to ensure that its Systems Assets/Resources and IT Processes are dependable, controlled and protected from misuse at all times. As part of the confirmatory process, it follows that all IT systems are audited at periodic intervals and a report on their status are submitted to Audit Committee of the Board.

Major objectives of the Information Systems Audit Policy:

- Safeguarding Information Systems Assets/Resources and IT Processes
- Verification of Data integrity and Security
- Evaluation of System effectiveness and efficiency:
- Verification of compliance to internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

a) Safeguarding Information Systems Assets / Resources and IT Processes:

Monitoring effective usage of Hardware, software, networking & communication facilities, people (Knowledge), system documentation, supplies etc

Evaluation of infrastructure (like Power, Air Conditioning, Humidity Control, physical security, Surveillance and monitoring, Incident monitoring etc) in safeguarding of I S Assets/Resources.

b) Verification of Data integrity and Security:

Validate that the data entered and captured in the system is duly authorised, verified and completed and that proper control is exercised at all stages viz. Data preparation, input, verification, output, modification, deletion, electronic transmission, etc. to ensure authenticity and correctness of data.

c) Evaluation of System effectiveness and efficiency:

Evaluate the extent to which the organizational goals, business and user needs have been met with and to determine whether resource utilization is effective and efficient in achieving the desired objectives.

d) Verification of compliance to internal guidelines & procedures in addition to legal, regulatory and statutory requirements.

Evaluate the level of compliance on

- adherence to maintenance of Integrity, Confidentiality, Reliability, Availability and Dependability of information resources;
- Legal, Regulatory and Statutory requirements,
- Internal Policy and Procedures based on prescribed standards and guidelines.

Scope of I S Audit:

The scope of I S audit includes the collection and evaluation of evidence / information to determine whether the Information Systems in use safeguards the assets, maintain data security/integrity/availability, achieve the organizational goals effectively and utilize the resources efficiently. It also includes the processes for the planning and organization of the Information Systems activity, the processes for monitoring of such activities and the examination of the adequacy of the organization and management of the I S specialist staff and non-specialists with I S responsibilities to address the I S exposures of the organization.

The I S audit covers all the computerized departments/offices of the Bank including CBS, Data Centre, DR Site and branches, ATM Switch, NEFT/ RTGS Cell, and any other new area of IT implemented / to be implemented by the Bank. In short, it includes all the activities/areas of the organization, where IT systems are used for business purposes.

I S Audit Methodology:

I. Identify the risks that the organization is exposed to, in the existing computerized environment and to prioritize such risks for remedial action.
II. Whether the implementation of Information Technology in the organization is as per the parameters laid down in the Information Security Policy and as duly approved by the Board of Directors.
III. Verify whether the Information systems policies have been devised covering various information assets for the entire organization and that the organization's systems and procedures and laid down I S security policies are adhered to.
IV. Verify whether the checks and balances prescribed by I S security policy and other relevant guidelines are strictly adhered to / complied with, towards risk mitigation through proper maintenance and prevention of abuse /misuse of I T assets and computer crimes.
V. Verify and comment on the level of checks and balances for ensuring compliance of laid down control measures.
VI. Adhere to the established norms of ethics and professional standards to ensure quality and consistency of audit work.

I S Audit Setup

Audit Charter:

The responsibility, authority and accountability of the information systems audit function, has to be appropriately documented in the engagement letter clearly defining the responsibility, authority and accountability of the IS audit function, for outsourcing of I S Audit.

The responsibility and accountability of internal I S auditors will be the same, as applicable to general inspecting officials as per the prevailing internal inspection/audit guidelines.

Independence:

To maintain the independence of I S Audit function (Inspection Department) from other departments and offices, its personnel shall report to Chief Executive Officer, who shall report to the Audit Committee of the Board (ACB).

Responsibilities:

The primary responsibility of the I S Audit is to achieve the objectives of the I S Audit function as enumerated in this policy document. In brief, the responsibilities of I S Audit function of the Bank is to

I. Identify and assess potential risks to the Bank's operations.
II. Assess the means of risk mitigation and safeguarding of IT assets
III. Review the adequacy of controls established, to ensure compliance with the policies, plans,

procedures, and business objectives.

IV. Assess the level of compliance to established procedures / controls
V. Assess the reliability and security of financial / management information and the systems and operations that provide this information.
VI. Assess the level of utilization of I T resources to understand their efficient and effective use for business growth.

Authority:

The Inspection Department / System, in the course of its I S Audit activities, is authorized to have unrestricted access to all areas of the bank, activities, documents, records, information, properties and personnel etc relevant to the performance of I S Audit function.

Require all members of staff and Management to supply such information and explanations as may be needed within a reasonable period of time to I S Audit staff, Heads of Department/ Branches should inform Inspection department/ system without delay of any significant incident concerning security and / or compliance with regulations and procedures.

Functions of ACB (Audit Committee of Board) on I S Audit related areas -

The Audit Committee should devote appropriate and sufficient time to I S audit findings identified during IS Audits and members of the Audit Committee would need to review critical issues highlighted and provide appropriate guidance to the Bank's management.

Accountability

(i) The Inspection Department shall prepare annual plan for I S audit covering all the computerized environments of the Bank viz. Branches / Offices /Departments etc, as per the periodicity prescribed in the Inspection & Audit Policy document. CEO through CISO IS Audit Cell shall place a periodic review report on the above to the ACB and follow up directions/ observations of ACB are for compliance.

External I S Audit firms:

The Bank may consider engaging the services of accredited External I S Audit firms for I S Audit of Branches / Offices / IT infrastructure including Netware Audit, software audit, Vulnerability Assessment, etc to meet any Business /Statutory requirements. Depending on the nature and criticality of assignment, the Bank may stipulate eligibility criteria of the External I S Audit firms, fees payable etc. The engagement letter should cover the scope of IS Audit, objectivity, duration etc apart from addressing the areas of responsibility, authority, and accountability.

I S Audit Policy Guidelines:

I S Audit activity is broadly divided into 5 major steps for the convenience and effective conduct of audit.

a) Planning I S Audit
b) Tests of Controls
c) Tests of Transactions
d) Test of Balances
e) Completion of Audit.

a) Planning IS audit:

Planning is the first step of the I S audit. I S auditors should plan the audit work in a manner appropriate for meeting the audit objectives. IS auditors are required to understand the internal controls used within an organization, like review of previous audit reports/papers, interview/ interaction with the management and Information Systems personnel, observation of activities carried out within the Information Systems function and review of Information Systems documentation.

In addition to the above, in case of outsourcing of I S Audit they should have an understanding of the audit department / office / organisation and its processes. It includes understanding of the objectives to be accomplished in the audit, collecting background information, assigning appropriate staff keeping in mind skills, aptitude etc. and identifying the areas of risk and to decide on the extent of the detailed analysis and testing to be conducted on those systems.

b) Tests of Controls:

Internal Controls are tested to evaluate the effectiveness of management and application controls. This will throw light on the level of reliability of the controls as per prescribed guidelines in the Information System Security Policy and find out weaknesses if any.

c) Tests of Transactions:

These tests are generally carried out using Computer Assisted Audit Tools /Utility Tools to assess the data integrity and computational accuracy of the transactions carried out. This will also bring out erroneous transactions, if any, leading to data abuse / misuse/ fraud with the help of transaction log available in the system.

d) Tests of Balances:

General Audit Software / expert systems can be used to assess the efficiency of system functioning and to estimate the losses that could have occurred during the failure of system safeguards in maintaining the data integrity, computational errors etc.

e) Completion of Audit:

This is the final stage of IS audit, where auditors will be recording their findings/observations, analysis and recommendations for necessary follow-up and monitoring for rectification/compliance by the concerned authorities. Potential IS audit findings should be discussed with the appropriate / authorized personnel throughout the course of IS auditing.

I S Audit of Branches /offices:

I. I S audit of branches shall be scheduled as per risk rating of the Branches under regular inspection (RBIA), wherein the I S Audit rating of the branch shall be dovetailed to RBIA rating format, as spelt out under Rating chart guidelines.

II. In the case of all other Offices/department/service providing centres which are not subjected to risk rating at present, IS audit shall be carried out along with the regular inspection, by the inspecting official as per the prescribed periodicity.

ATM Audit / ATM review

1. All Off- site and on-site ATMs shall be subjected to either ATM audit or ATM review once in 12 months. However, ATMs attached to branches with Concurrent / Internal Auditor shall be

subjected to quarterly review.

2. Audit of ATMs connected to our Branches shall be carried out along with Regular inspection of branches (RBIA), while ATM review shall be conducted by Concurrent auditors.

I S Audit of Third-party IT environments – Bank shall subject IT environments of third parties (service providers) to I S Audit by our Banks' Internal auditors or by External auditors depending up on the complexity of the environment, to verify / satisfy about safety & security of information assets of the bank in the hands of third-party vendors.

Authorities Responsible to conduct I S Audit, Review & follow up of audit reports.

The guidelines for conducting I S Audit, authorities empowered to conduct the audit / review the reports/ closure of reports etc shall be as per the I S Audit procedures document and as per the periodicity detailed in the enclosed annexure.

I S Audit schedule and cycle:

The checklist based I S Audit of Branches (including new branches opened /to be opened) shall be carried out along with regular inspection of the Branch and I S audit rating arrived shall be dovetailed, as spelt out under Rating chart guidelines.

Follow up and closure of IS Audit reports.

The inspecting official submits the report immediately on completion of the assignment and the report reaches the Branch/Zonal Office/IC concerned within 3 working days.

The following is an illustrative list, warranting special reports:

- Lack of awareness in maintaining password secrecy;
- Non-checking of Single window operator (SWO) report/ e-VVR with physical vouchers on daily basis;
- Non-checking of exceptional / Override report / other branch transactions on a daily basis by Branch in charge;
- Maintenance of Parking a/c in branches, other than those permitted by the system;

Rating Of Branches under IS Audit:

Evaluation of performance and functioning of a Branch based on I S Audit findings through a system of Rating, is an important tool to assess vulnerability and threat associated with the IS activities of the branch. This Rating has a bearing on the performance of Branch Manager and other officials and staff. Hence, an objective system of rating is developed based on the risk perception associated with the various I S activities, mainly through the concept of IS audit around the computer, to start with. The Inspecting Official is required to use the same to effectively evaluate the use of I S assets for effective performance and functioning of a branch.

Rating system under IS Audit:

The following ratings will be awarded under IS Audit functioning based on adherence to various guidelines by the branch in safeguarding the IS Assets of the bank in addition to effective and efficient use of IS Assets.

Below 50% - High Risk

Between 50 and 70% - Medium Risk

Above 70% - Low Risk

A Branch will be rated as "High Risk" either for scoring below 50% marks, OR for not scoring full marks under identified 'Compulsory scoring items' as indicated in the I S rating chart (due to non-adherence/ non-compliance of various guidelines under IS Audit).

Inspecting official has to discuss the rating given by him with the Branch Manager concerned, on completion of I S Audit and finalization of the report.

UIDAI/Aadhaar related Policy:

Following portion of the document illustrates the Policy of the bank related to UIDAI/Aadhaar.

Uttarakhand State Co-Operative Bank will comply with all Information Security Policy and Procedures addressing the security aspects of Aadhaar as defined under the Aadhaar Act, Regulations and specifications.

Certain Specific Processes/Policies are defined below:

I. Bank will take the consent of Aadhaar Card Holder for Authentication and save the consent forms with the consent details for a period of atleast 7 Years. Similarly, the logs regarding Authentication will be saved for 2 years Online and 5 years Archived.

II. For any given Aadhaar number holder, whose identity information was collected, the bank will be able to demonstrate that consent was taken and disclosure of information was made whenever required for any Regulatory requirement.

III. Aadhaar card holder will be intimated when the request for NPCI mapping of account number has been initiated by Uttarakhand State Co-Operative Bank via SMS/Email in 24 Hours.

IV. Uttarakhand State Co-Operative Bank will Whitelist any applications (Web/ Android/ iOS or any other client applications) in public domain with Uttarakhand State Co-Operative Bank's name, application name, logo and URL etc.

V. Uttarakhand State Co-Operative Bank shall be fully responsible for the misuse and illegal sharing of the license key in production or pre-production environment of UIDAI. Uttarakhand State Co-Operative Bank shall not allow any other agency to perform authentication by sharing its license key. Uttarakhand State Co-Operative Bank shall not forward authentication request using PID block captured by unaudited application using their license key. For every sub-AUA if any, a separate license key shall be used.

VI. Uttarakhand State Co-Operative Bank understands that in case, Authority notices misuse or illegal sharing of license key by the AUA / KUA / sub-AUA, Authority shall terminate the license of the AUA / KUA and other actions including criminal prosecution shall be taken against AUA / KUA as well as the sub AUA and other entities as per Aadhaar Act and its Regulations.

VII. Uttarakhand State Co-Operative Bank shall not perform any test transactions on UIDAI's production environment. Any test transaction will be performed on UIDAI's pre-production environment only.

VIII. In all authentication applications deployed by Uttarakhand State Co-Operative Bank and sub-AUA, name of Uttarakhand State Co-Operative Bank shall be clearly displayed to the Aadhaar number holder.

IX. Uttarakhand State Co-Operative Bank shall ensure that it has provisions for periodic reviews and assessments of its systems, infrastructure, etc., by a UIDAI empanelled or CERT-In

empanelled agency to ensure compliance with Aadhaar Act, Regulations and specifications on annual basis or as defined by UIDAI.

X. As a part of the Exception handling process if fingerprint is not working at all then alternate option of iris or OTP will be provided for Aadhaar Authentication.

XI. Uttarakhand State Co-Operative Bank will comply with Regulation number 23, Chapter-III, Aadhaar (Authentication) Regulations, 2016 in case it wants to surrender its UIDAI License keys.

XII. Uttarakhand State Co-Operative Bank will ensure that Team working on Aadhaar based applications development is aptly qualified (Graduate is Minimum requirement).

XIII. Uttarakhand State Co-Operative Bank will comply with all the requirements of UIDAI Circular No. 06 of 2018, K- 11020/217/2018-UIDAI (Auth-I), dated 04th June 2018 (Implementation of Virtual ID, UID Token and Limited KYC) by implementing the latest Authentication API 2.5, EKYC API 2.5 and OTP Request API 2.5 for VID and UID Token.

XIV. Uttarakhand State Co-Operative Bank will comply with all the circulars, notices, mandates issued by UIDAI from time to time.

As an AUA, Uttarakhand State Co-Operative Bank understands and will always follow any of the following Do's and Don'ts related to UIDAI/Aadhaar Applicable to it as stipulated by UIDAI:

Do's:

1. Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
2. Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc issued by UIDAI from time to time.
3. Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.
4. Follow the information security guidelines of UIDAI as released from time to time.
5. Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
6. Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.
7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored.
8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.
9. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number-based index.
10. Regular audit must be conducted to ensure Aadhaar number and linked data is protected.
11. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.
12. An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.

13. Identify and prevent any potential data breach or publication of personal data.
14. Ensure swift action on any breach personal data.
15. Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
16. Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.
17. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure all Aadhaar holders are able to use it effectively.
18. Multi-factor for high security - When doing high value transactions, multifactor authentication must be considered.
19. Create Exception handling mechanism on following lines
20. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.
21. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.
22. If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.
23. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.
24. All authentication usage must follow with notifications/receipts of transactions.
25. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, sms, physical-center, etc.).
26. Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.
27. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

Don'ts:

1. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
2. Do not store biometric information of Aadhaar holders collected for authentication.
3. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
4. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed.
5. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar act. The purpose of use of Aadhaar information needs to be disclosed to the resident.
6. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
7. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
8. Do not permit any unauthorized people to access stored Aadhaar data

9. Do not share Authentication license key with any other entity.

Compliance:

Bank's IS Audit policy generally conforms to "Information Systems Audit Policy for the Banking and Financial Sector" of Reserve Bank of India and latest RBI working group guidelines on electronic banking and information security published in April 2011. Whenever a specific mention is not made here in, details provided in RBI guidelines mentioned above, shall hold good as far as it is applicable to the environment.

Inspecting officials shall ensure that the branches/ offices using IT Infrastructure are strictly adhering to the various guidelines issued by Head office (CISO) from time to time.

CEO with the assistance of CISO (IS Audit cell), may devise / modify the reporting formats for Information Systems Audit, as and when required.

Inspecting officials shall ensure that the branches/offices using IT infrastructure are strictly adhering to the various guidelines issued by IS security Cell and IS Audit Cell from time to time, apart from the manuals like present guidelines on Information Systems Audit.