INDRAPRASTHA SEHKARI BANK LIMITED
इंद्रप्रस्थ सहकारी बैंक लिमिटेड

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

VERSION CONTROL DOCUMENT

Policy No.	33
Policy Name	Operational Risk Management Framework & Operational Resilience
Version No.	1.0
Board Resolution Date	26.03.2025
Board Resolution Number	14
Review Date	-
Next review date	01.04.2026 (or earlier if there are any changes)
Classification	Confidential for Internal Circulation only

Version Control Information:

Version No.	Date Issued	Author	Update Information
1.0	26.03.2025	Head Office	

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

Operational Risk Management Framework & Operational Resilience

Preliminary: Operational risk management (ORM) is the process of proactively identifying, assessing, mitigating, and monitoring risks that disrupt daily operations. These risks can be internal, such as people, processes, and systems, or external, like natural disasters or regulations.
An Operational Risk Management Framework (ORMF) is a structured approach that helps businesses proactively identify, assess, prioritize, monitor, and report operational risks whereas Operational Resilience provided the ability to deliver critical functions in the event of any disruption.

1 - Operational Risk: Operational risks mean potential losses arising from failures within bank's internal processes, systems, or people, including issues like system glitches, employee errors, fraud (internal and external), compliance breaches, business disruptions, cyber-attacks, data breaches and inadequate risk management practices, all of which can impact the bank's normal operations, financial stability and reputation.

2 - Operational Risk Management Process (ORMP): ORM process at the Bank involves identification, assessment, mitigation and reporting of risk information to the senior management and the Board of Directors through various Sub-Committees of the Board. The process of risk management at the bank starts with the top management and adhered to by the bottom line. The procedure heavily relies on data consistency and accuracy. As such, the bank shall ensure well-defined processes for identifying, assessing, and monitoring key operational risk exposures.

2.1 Principles of Risk Management: The risk management process at the bank involves six components:

2.1.1 Risk Identification: The Bank shall ensure comprehensive identification and assessment of the operational risk inherent in all its material products, activities, processes and systems. Both internal and external threats and potential failures in people, processes and systems shall be assessed promptly and on an ongoing basis.

2.1.2 Risk Assessment: Assessment involves quantification of the impact (to the extent possible) of risks to determine potential severity and probability of occurrence. Each identified risk is assessed on two factors which determine the risk exposure i.e. its potential impact and likelihood of occurrence/recurrence. After taking into account the existing controls, the risks are assessed to ascertain the current level of risk, and categorization of risks as – low, medium and high.

2.1.3 Mitigation of Risks: All the identified risks shall be mitigated by using any of the following risk mitigation plans:

a) **Risk avoidance**: by not performing an activity that could carry risk. However, such avoidance can result into losing out on the potential gain that accepting (retaining) the risk may be allowed;

b) **Risk Transfer**: The process of formally or informally shifting the financial consequences of particular risks from one party to another.

c) **Risk reduction**: Employing methods/solutions that reduce the severity of the loss.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

d) **Risk Retention**: Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of insuring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred are retained by default.
e) **Risk Awareness**: Raising awareness about managing risks across the organization.

2.1.4 Monitoring and reviewing risks: Risk monitoring, reviewing, mitigating and reporting are critical components of risk management process. The bank shall conduct Risk Reviews that are needed for effective risk management regularly. The Bank periodically reassess its risk levels in order to ensure how well the risk strategies function and also update risk models.

2.1.5 Risk Appetite: Risk appetite is the amount of risk the bank is willing to take in pursuit of objectives. It is the risk capacity or the maximum amount of residual risk that it will accept after controls and other measures have been put in place.

3. Dimensions of Operational Risk & control gaps:

Inherent Risks	**Control Gaps**
KYC non-compliance	System to monitor KYC compliance
Internal Accounts	Policy/Controls in Internal Accounts
Suspicious transactions	Mechanism for identification of suspicious transactions
Audit compliance	Timeliness and sustenance of audit compliance
Frauds	Strengthening internal controls
Third party dependency	Review of outsourcing arrangements.

3.1 Operational Risk Governance: The Operational Risk Management and Operation resilience at the bank has been built on three pillars. These are - Prepare & Protect, Build Resilience and Learn and Adapt. The ORM function at the bank has been built on a three-layered defence, as under:

OPERATIONAL RISK MANAGEMENT AT THE BANK – THREE PILLARS

PILLAR 1; Prepare & Protect	**Pillar 2: Build Resilience**	**Pillar 3: Learn and Adapt**
• Governance & Risk Culture • Responsibilities of Board of Directors & Senior Management • Risk Management Identification & Assessment • Change Management • Monitoring & Reporting	• Formulation of Policies & Procedures with the approval of Board of Directors. • KYC, AML, CFT risk framework • Business Continuity Planning and Testing • Mapping Interconnections &	• Disclosures & Reporting • Lessons Learned Exercise and Adapting • Continuous Improvement through Feedback Systems

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

• Control & Mitigation	Interdependencies • Third Party Dependency Management • Incident Management • ICT including Cyber Security • Fraud Risk Management	

PILLAR – 1,
PREPARE & PROTECT – Three lines of defence for management of operational risks

First Line – Internal Control Framework

Identification – Identify sources of risk, events & their potential consequences;
Assessment – Assess the causes and sources of risk and causes of recurrence of such risks;
Evaluation - to determine how low or high the probability of occurrence is and how severe the consequences are
Manage – Execution of control measures.
Monitoring & Review - Continuously monitor the effectiveness of controls and measures
Review and update risk assessments to stay ahead of emerging risks

Second line of Defence – Bank's ORM Function

Bank's operational risk management function forms the second line of defence.

- Developing and maintaining Operational Risk Management and measurement policies, standards and guidelines;
- Reviewing and contributing to the monitoring and reporting of the Operational Risk profile; a
- Designing and providing Operational Risk training and instilling risk awareness, and
- Compliance - The Senior Management / Board shall ensure compliance of various policy guidelines.

Third Line of Defence – Audit Function

Audit function at the bank provides an independent assurance to the Board regarding the appropriateness of bank's ORM.

The internal/External auditors shall carry out review of the above two lines i.e. internal control and compliance covering all activities at the bank.

3.2 It has been ensured that each line of defence at the bank:

- has clearly defined roles and responsibilities;
- is adequately resourced in terms of budget, tools and staff;
- is continuously and adequately trained;
- promotes a sound operational risk management culture across the bank; and
- communicates with the other lines of defence to reinforce the ORMF.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

PILLAR – 2, BUILD RESILIENCE

Key aspects considered at the bank for building resilience:

- Compliant KYC, AML & CFT framework
- Comprehensiveness of policies
- Credit Risk Management
- Continuous monitoring of HR related functions
- Effectiveness of measures to deal with grievance redressal process etc.
- Controls related to out-sourcing
- Effectiveness of Fraud Risk Management
- Robustness of CBS systems
- Robustness of Data reporting
- Effectiveness of IT and cyber security controls
- Business continuity planning and testing
- Incidence response & recovery plans
- Technology Vision and
- Overall regulatory compliance

PILLAR – 3, LEARN AND ADAPT

Disclosures & Reporting – Bank's public disclosures may allow stakeholders to assess its approach to Operational Risk management and its Operational Risk exposure. The Bank shall have a formal disclosure policy subject to regular and independent review and approval by the Senior Management and the Board of Directors, respectively.

Lessons learned exercise and adapting - A lessons learned exercise shall be conducted after a disruption to a critical or important business service to enhance the bank's capabilities to adapt and respond to future operational events.

Continuous improvement through feedback systems – The Bank shall promote an effective culture of learning and continuous improvement as operational resilience evolves through effective feedback systems on an ongoing basis.

4. Risk Governance: The Board of Directors shall be responsible for managing comprehensive risks. Various sub-committees, constituted by the Board, oversees the implementation of the risk strategy and guides the development of our policies, procedures and systems besides evaluating their adequacy and appropriateness to the changing business conditions, as well as our risk appetite. The Chief Executive Officer (CEO) interacts regularly with the members of the Sub-Committees who are primarily responsible for implementing the risk strategy approved by the Board, and developing policies, procedures and systems for identifying, measuring, monitoring, assessing and managing risks.

The Bank shall review and revise its policy documents, as appropriate, based on continued assessment of the quality of the internal & external control environmental changes or on occurrence of a material change in the Operational Risk Profile of the Bank.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

4.1 Role of Board of Directors: The Board of directors of the bank will have an oversight on all the risks assumed by the bank with specific Sub-committees of the Board constituted to facilitate focused risk management. The Board of Directors shall approve and periodically review:

- implementation of various policies, processes and systems of risk management at all levels.
- the risk appetite and tolerance levels.
- regularly review and evaluate the effectiveness of, and approve the ORMF to ensure the bank has identified and is managing the internal & external Operational Risks.

4.2 Role of Senior Management: Senior Management shall develop for approval by the Board of Directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. The Senior Management shall be responsible for-

- consistently implementing and maintaining throughout, bank's policies, processes and systems for managing Operational Risk in all material products, activities, processes.
- Bank's activities are conducted by staff with the necessary experience, technical capabilities and access to resources.
- Staff responsible for managing Operational Risk co-ordinate and communicate effectively with staff responsible for managing credit, market, and other risks, as well as with those who are responsible for the procurement of external services.

4.3 Key areas of Operational Risk: The nature of our business and business activities, along with the regulatory environment and external environment at large, exposes us to several types of risks. For us, the key risks are KYC related, credit risk, market risk, liquidity risk, operational risk, cyber security and data risk. Our operations expose us to compliance and reputation risk also.

4.3.1 Know Your Customer (KYC) policy: In terms of updated Master Directions on KYC-2016, the Bank has in place a policy framework on Know Your Customer (KYC) norms and Anti-Money-laundering measures. The Bank is following the Reserve Bank of India (RBI) guidelines, which include Customer Acceptance Policy, Customer Identification Procedures, Monitoring of Transactions, and Risk Management, and periodically update KYC information. The Bank has adopted a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk. However, periodic updation shall be carried out at least once in every two years for high-risk customers, once in every eight years for medium risk customers and once in every ten years for low-risk customers from the date of opening of the account / last KYC updation. In nut-shell, the bank has ensured:

- All KYC / AML / CFT guidelines implemented at the bank;
- Periodic KYC updation
- Broad principles for Risk categorization of customers
- Beneficial ownership details
- Deduplication of UCIC
- Officially Valid Documents (OVDs) captured in CBS
- Uploading KYC data with Central KYC Registry
- Politically exposes persons (PEPs) and enhanced monitoring
- On-going due diligence
- Reporting requirements to Financial Intelligence Unit (FIU-IND) are complied with;
- Details of accounts resembling any of the individuals/entities in the lists, if any, are being reported to FIU-IND apart from advising Ministry of Home Affairs (MHA) as required under UAPA.
- 'UNSCR 1718 Sanctions List of Designated Individuals and Entities' as amended from time to time, is being verified regularly while onboarding new customers.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

4.3.2 Cash & Clearing Management: Consequences of financial and non-financial improprieties arising out of non-compliance with laid down systems & procedures and or non-adherence to the 'due-diligence' norms as per service & conduct rules of the Bank are firmly dealt with. The term 'Financial Impropriety' includes but not limited to the following:

- cash shortage not reported on day of occurrence by cash handling officials,
- misappropriation and criminal breach of trust
- Detection / Impounding of Counterfeit Notes
- collection of an instrument which is genuine but the amount collected fraudulently by a person who is not the true owner, any negligence of the dealing officials if the Bank is acting as collecting banker;
- Collection of altered or fake cheque and in the event such fake/altered cheque having been paid/encashed etc.

The Bank has ensured adequate controls and safeguards to prevent, detect, or correct operational risks in cash and clearing management activities and processes, as under:

- Cash held in branch safe and strong room is always under dual custody of the Branch Manager and dealing official (Cashier).
- The cash safe/strong room shall be locked by the joint custodians, so that no, one official singly can open the cash safe/strong room. The bulk of the Cash Balance shall always be in the Strong Room / Cash Safe under joint custody.
- The Joint Custodian of cash (i.e. Manager / authorized supervising official as the case may be) shall check the cash every time before depositing the same in the strong room safe.
- Sample checking of coins and small coins is also ensured. Visiting senior officials / internal auditors ensures physical checking of cash on their visits to the branches.
- Apart from the daily check of cash and surprise check of cash at least once a month, the entire cash in a Branch/Vault shall be verified by an official unconnected with custody of cash.
- Officials entrusted with the Bank's keys shall take proper care of the keys at all times, ensuring that the principle of "Dual Control" is always maintained and that the keys are not handed over or made accessible to any unauthorised person. In case any of the joint custodians goes on leave, keys are handed over to the next authorized official under proper record.
- Remittance/transfer of cash is ensued by bank's own van accompanied by armed guards.
- Necessary infrastructure and processes are in place to facilitate the clearing, settlement of financial transactions besides ensuring reconciliation of bank statements on daily basis. Excess cash beyond permissible limits, is timely lifted from branches and remitted to linked current chests.

4.3.3. Inoperative Accounts/Unclaimed Deposits: The bank shall ensure that there is no unauthorised access to customer data pertaining to the inoperative accounts. The bank shall also ensure that adequate steps are taken to prevent data theft and related misuse of such accounts for fraudulent purposes. Accordingly, in terms of extant RBI guidelines on Inoperative Accounts and Unclaimed Deposits, the Bank has developed a Standard Operating Procedure (SOP) for implementation at all branches to mitigate the embedded risks, which include:

- Annual review in case of no customer induced transactions for more than a year
- Alert messages to customers to activate the account in one year
- Review term deposit accounts which have not been renewed or transferred on maturity
- Monitoring of accounts and concurrent audit after re-activation for at least six months
- Tracing of Customers of Inoperative Accounts / Unclaimed Deposits
- Levy of charges
- Fraud Risk Management and
- Customer awareness measures.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

4.3.4 Transfer of unclaimed deposits to DEA Fund: Bank shall deposit the credit balances in deposit accounts maintained with the bank and which have not been operated upon for ten years or more, or any amount remaining unclaimed for ten years or more shall be transferred to the DEA Fund in the specified account maintained with the Reserve Bank. Bank has ensured:

- Timely submission of prescribed returns to RBI
- Returns are subjected to verification by Statutory Auditors
- Disclose the amounts transferred to DEAF under the notes to accounts as prescribed
- Display of inoperative accounts of more than 10 years on bank's website/public domain
- Bank has provided a search facility option for benefit of public
- Bank has allotted a UDRN (Unclaimed Deposit Reference Number) for each unclaimed deposit transferred to the DEA Fund.

4.3.5 Internal Accounts: The Bank ensures regular monitoring of internal accounts through:

The office account(s) are created by banks to park funds for a brief period before being credited to the intended account holder's account. Due to lack of defined purposes for internal/office accounts and unrestricted access for making inappropriate entries, this could lead to operational inefficiencies, manipulation and frauds resulting in financial losses. The Bank has ensured appropriate checks and controls and implemented corrective measures to prevent unauthorized operations in internal/office accounts.

- Banks shall clearly define the purpose of each internal/office account to ensure proper usage and prevent misuse.
- Implement strict access controls to prevent unauthorized individuals from making entries or transactions in internal/office accounts.
- Regularly monitor internal/office account transactions to detect any suspicious activities or unauthorized operations.
- Conduct regular internal audits of internal/office accounts to identify any weaknesses in controls and procedures.

4.3.6 Effectiveness of CBS: The Bank is using Cloud based Core Banking System implemented by M/s. Stellar Informatics P. Ltd. in SaaS Mode. The bank focuses on enhancing the end-point security, network security, server security, data-base and application security to protect the customer financial information. The Bank has deployed quality manpower for handling IT and MIS related matters. Some of the security features of the CBS at the bank are as under:

- **Data Security**: Employed strong encryption techniques, implemented data protection measures for customer protection and regulatory compliance.
- **Access Control:** include role-based access control, security user authentication protocols and mechanisms to restrict access to sensitive data to authorized personnel only, two-factor authentication.
- **Network Security**: protecting CBS from external threats and unauthorized access, intrusion detection and prevention systems, firewalls and network segmentation to isolate the CBS and protect it from potential threats. Regularly updating the CBS and its underlying infrastructure with latest security patches.
- Assessing and addressing vulnerabilities promptly.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

- **Security Monitoring and Logging**: Real time monitoring tools to detect and respond to security incidents, maintaining comprehensive logs of all system activities, regular back-ups of CBS data and system configuration.
- **Change Management**: The Bank has put in place a change management process to record/monitor all the changes that are moved / pushed into production environment.

4.3.7 Customer Service: Operational risks in bank customer service stem from inadequate processes, systems, people, or external events, potentially leading to financial losses, reputational damage, and customer dissatisfaction. In order to mitigate the risks in customer service, the bank has:

- constituted a Customer Service Committee
- Adopted Fair Practice Code
- coverage of customers under Nomination Facility
- Support comprehensive Notice Board – display of information
- Toll free number for lodging complaints/reporting and blocking lost cards
- Registration of mobile numbers/e-mail Ids of customers for sending alerts
- Limited Liability of a Customer in electronic banking transactions.

4.3.8 Credit Risk: Credit is the core activity of the bank which forms an important source of bank's earnings. Credit risk is found in all activities where success depends on counter party, borrower or guarantors' performance. Asset quality of the bank depends upon proper risk assessment at the beginning of any loan proposal.

Mitigation: The bank has put in place loan policy which focuses on the following points:

i. The Bank has well defined loan policy which is reviewed on a yearly or earlier in case fresh guidelines received from the RBI;

ii. Loan policy clearly defines strategies for distribution of credit to different sectors of the economy and to strengthen the credit appraisal & monitoring system.

iii. The bank ensures entry check points while sanctioning the credit proposal. Business feasibility, sustainability of business in the long run, quality of management, past track record of performance, adequate security and margins etc has been evaluated during the credit appraisal procedure.

iv. Delegation of powers down the line to executives and Loan committee for speedy disposal of credit. The bank has build-up, appropriate credit delivery system with adequate delegation of authority along with responsibility and accountability.

v. Credit appraisal system comprises of thorough assessment of borrower's activity, CMA data analysis, ratio analysis, need based requirement, viability of the project based on well-defined norms for credit assessment.

vi. Credit Rating is an evaluation of the creditworthiness of a borrower to fulfil financial commitments or repayment of debts and other financial obligations.

vii. Loans Department shall monitor the credit portfolio in the bank on a monthly and quarterly based reporting to the CEO.

viii. The guidelines issued by RBI in respect of classification and maintenance of priority sector advances are strictly followed by the loan officials by issuing various circulars to the branches for implementation.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

ix. Prudential norms on Income Recognition, Asset Classification, and Provisioning pertaining to advances, by classifying them under SMA categories as prescribed are in place and reviewed by the Board.

x. Monitoring the end use of funds to ensure use of banks funds as intended, preventing diversion and reducing risks.

xi. Dealing officials are being imparted trainings at regular intervals.

4.3.9 Fair Lending Practices: In terms of RBI guidelines aimed at fostering fairness and transparency in lending practices, the bank has ensured:

- Interest may be charged only from the date of disbursement
- Release of Movable / Immovable Property Documents
- Display of information of secured assets possessed under SARFAESI Act
- Key Facts Statement (KFS) to all new retail and MSME term loans to enable borrowers to make well-informed financial decisions.
- Board approved policy on penal charges
- Framework of compensation to customers for delayed updation / rectification of credit information – strengthening of customer service.

5. OTHER RELATED RISKS:

5.1 Market Risk: The risk of potential loss on account of adverse changes in market variables which affect the value of financial instruments such as debt securities held by the Bank for management of statutory reserves.

Mitigation - A well-defined Board approved Investment Policy is in place. The bank has ensured robust internal credit rating system in respect of investments, which include building up of a system of regular (quarterly or half-yearly) tracking of the financial position of the issuer to ensure continuous monitoring of the rating migration of the issuers/issues. The Bank may diversify its existing portfolio by adding securities whose value is less prone to interest rate fluctuations of funds, from time to time. The Committee also evaluate the pricing of deposits and advances products, keeping in mind the cost of funds to the Bank, yield on advances and investment of SLR and Non-SLR funds viz-a viz steep downfall in operating profits of the Bank.

5.2 Interest Rate Risk: Interest Rate Risk is the risk where changes in market interest rates might adversely affect the Bank's financial condition. Impact of interest rate movement has its impact on Net Interest Margin of Bank.

Mitigation: The Bank has adopted Interest Rate Sensitivity statement (IRS) as prescribed by RBI with eight buckets. The IRS statement would be prepared on quarterly basis and present to the Board with ALCO recommendations. Risks such as embedded option risk, re-investment risk, credit default risk are being carefully looked into by the ALCO.

5.3 Liquidity risk - is the risk to earnings or capital which arises from a bank's inability to meet its obligations when due without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned decreases or changes in funding sources. Liquidity risk exposure is present in various funding situations, but primarily deposit and lending activities.

Mitigation: The Bank has classified its retail deposits in the appropriate time bands on the basis of their behavioural maturity rather than residual maturity. However, inter-bank deposits, Certificate of deposits &

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

bonds etc. have been put under their respective residual time band. Short-term dynamic liquidity statements are prepared and discussed. Mis-match in liquidity is being thoroughly examined to ascertain the causes and to alleviate the impact. The bank focus on short-term mismatches and monitor its cumulative mismatches across all time-bands by establishing internal prudential limits duly approved by the ALCO/Board. Statement on structural liability is also prepared on quarterly basis placing all the cash flows and out-flows in the maturity ladder.

Overall, the Investment and Asset-liability Management policy has been documented focussing on:

i. All SLR and Non-SLR investments are being transacted as per delegated powers by the officials.
ii. CRR/SLR are being maintained as per regulatory norms by the Funds Management Committee;
iii. Bank manages interest and market risk to earn additional income while maintaining surplus of assets over liabilities.
iv. Monthly valuation of SLR and Non SLR investments.
v. Additionally, balances are also being maintained with RBI.
vi. The Bank has made arrangements of overdraft facility against fixed deposits with other banks in case of liquidity fall back arrangement situation.
vii. The Liquidity position is prepared daily and placed before CEO of the bank.
viii. Ensuring daily Cash Management of Branches.
ix. Interest-Sensitive GAP Analysis will be prepared for market risk mitigation.
x. the Committee shall meet at least once in a quarter, to discuss Assets/Liability Management issues viz-a-viz Statement of Structural Liquidity, Statement of Interest Rates Sensitivity and Statement of Short-Term Dynamic Liquidity.
xi. ALCO shall consider the Maturity Profiles to measure the future Cash flows in different time-bands.
xii. Reviews are put up to the Board at quarterly intervals.

5.4Compliance Risk: Is the risk of legal or regulatory sanctions, material financial loss or loss of reputation, the Bank may suffer, as a result of its failure to comply with laws, regulations, rules and codes of conduct etc. applicable to its activities. Compliance function shall ensure strict observance of all statutory and regulatory requirements for the Bank, including standards of conduct, managing conflict of interest, treating customers fairly and ensuring the suitability of customer service.

Mitigation: To manage compliance risk, the bank shall adhere to Reserve Bank of India (RBI) guidelines, which include implementing robust internal controls, monitoring transactions, and staying updated on regulatory changes, with non-compliance leading to penalties and reputational damage. Key RBI Compliance Requirements

- IT Governance: Implement robust policies for data security and risk management.
- Data Protection: Enforce data localization and secure data-sharing practices.
- Vendor Management: Conduct thorough risk assessments for third-party vendors.
- Incident Response and Disaster Recovery.

The bank has put in place KYC – AML, a critical component of compliance, to detect and prevent money laundering and terrorist financing activities. This includes implementing customer due diligence (CDD) measures, conducting ongoing monitoring of customer accounts, and reporting suspicious activities to the relevant authorities.

The senior management shall ensure enhanced due diligence, employee training and automated tools to strengthen compliance risk besides carrying out an exercise to identify and assess the major compliance

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

risks and formulate remedial plans. The compliance function is subjected to concurrent / internal audit at the Bank.

6. Fraud Risk Management: The bank has put in place a structure of rules, practices and process in the form of a policy document on Fraud Risk Management System in terms of revised/updated directives of the RBI specifying role of the Board, Board Committees and Senior Management.

6.1 Fraud Risk Governance: The Bank has constituted a Committee of the Executives (CoE) headed by the Chief Executive Officer and two senior officers of the Bank for the purpose of performing the roles and responsibilities of 'Special Committee of the Board for Monitoring and Follow-up of cases of Frauds'(SCBMF) who shall oversee the effectiveness of the fraud risk management in the Bank.

The CoE shall review and monitor the incidence of frauds, including root cause analysis, and suggest mitigating measures for strengthening the internal controls, risk management framework and minimizing the incidence of frauds. The coverage shall include, among others, categories/trends of frauds, industry/sectoral/ geographical concentration of frauds, delay in detection/classification of frauds and delay in examination/conclusion of staff accountability, etc. Corresponding reviews shall be placed before the Board/Audit Committee of the Board at quarterly rests.

Detailed guidelines on Modus Operandi, Root-Cause Analysis of all major frauds and weaknesses in Due Diligence and Monitoring Measures, as analysed by the RBI, have been issued for compliance at all the branches of the bank.

Whistle Blower Policy – Whistle blower complaints on possible fraud cases / suspicious activities in accounts shall be examined at the bank.

7. Technology and Cyber Security Risk Management: To manage Technology and Cyber Security risk bank has implemented prescribed baseline cyber security and resilience requirements. The Bank has put in place IT policy, Comprehensive Cyber security policy, Incidence Management & Response System and Outsourcing/Vendor Management measures.

Mitigation:

- Implemented bank specific email domains with anti-phishing and anti-malware, DMARC controls enforced at the email solution.
- The bank's Information Technology sub-Committee ensures that Information Technology strategy is aligned with the business strategy.
- Review ongoing IT projects and their schedules.
- Major IT incidents, technology risk indicators and status of regulatory compliance,
- Policies and control framework on change management and Logical access management.
- The bank has ensured audit of Gap assessment of Comprehensive Cyber Security Framework of RBI by a Cert-In empanelled auditing firm.
- IS Audit periodically to provide assurance on the effectiveness and efficiency of IT systems and processes.
- Cyber incidents, if any, shall be reported on DAKSH portal within 6 hours of detection.
- VAPT audit is also being conducted of hardware, software and networking assets. System audit has also been conducted in compliance of RBI guidelines.
- The bank's Information Technology Committee oversees cyber security related threat landscape and bank's preparedness to address these from a prevention, detection and response perspective.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

- The IT Department will be responsible for tracking the risks. Confidentiality, Integrity and Availability of data form part of a comprehensive information security framework that the bank has put in place.
- The Bank has also set up an out-sourced Security Operations Centre(C-SOC)
- The Cyber Crisis Management Plan at the bank analyze the scope of cyber incidents, policies, actions and responsibilities for a coordinated approach to mitigate and recover from malicious cyber related incidents
- The Bank has subscribed to anti-phishing and anti-rogue application services, a solution designed to protect individuals and organisations from phishing attacks and rogue websites.
- The Bank has put in place a Vendor/Outsourcing Risk Management Policy. The bank thoroughly satisfy itself about the credentials of vendor/third-party personnel accessing and managing the UCB's critical assets. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third-party service providers.
- The Bank shall ensure timely renewal of such agreements. The Bank shall also seek VA / PT report as well its compliance from its third-party CBS providers or a certificate shall be asked for in this regard. The Bank shall also undertake vendor reviews which shall be put up to the Board.

7.1 Digital Intelligence Platform: The Bank has also on-boarded on the Digital Intelligence Platform (DIP) developed by the Department of Telecommunications (DoT). It is a secure and integrated platform for real time intelligence sharing, information exchange and coordination among the Telecom Service Providers, law enforcement agencies, banks and financial institutions, social media platforms, identity document issuing authorities etc.

The bank will also lay emphasis on customer elements and shall invest in areas of phishing protection, adaptive authentication, and awareness initiatives and will also take industry-leading initiatives in providing customers with an easy and immediate ability to configure their risks and limits.

7.2. Business Continuity: BCP forms a part of Bank's overall Business Continuity Management (BCM) plan, which is the "preparedness of the Bank", which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes, at an agreed level and limit the impact of the disaster on people, processes and infrastructure (includes IT); or to minimise the operational, financial, legal, reputational and other material consequences arising from such a disaster. Board of Directors has the ultimate responsibility and oversight over BCP activity of the bank.

7.3 Citizen Financial Cyber Frauds Reporting and Management System (CFCFRMS) – The Bank has onboarded on CFCFRMS platform (a portal of NCRP) developed by Indian Cyber Crime Coordination Center, (I4C) Ministry of Home Affairs where State Law Enforcement Agencies register complaints using helpline number 1930 in their respective states. The system is functional across the country and more than 200 intermediaries that includes Banks, Small Finance Banks, Payment Aggregators/Gateway, E-Commerce Companies etc.

7.4 Information and Communication Technology (ICT) including Cyber Security: Effective ICT performance and security are paramount for the Bank to conduct its business properly. The appropriate use and implementation of sound ICT risk management contributes to the effectiveness of the control environment and is fundamental to the achievement of strategic objectives. Based on information and/or systems classification, equipment shall be protected to reduce risks from environmental threats and hazards and to reduce the risk of unauthorized access to information.

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com

7.5 Advisories & Alerts received from regulators: Extant RBI guidelines, advisories and alerts received from the regulators are being immediately taken-up for compliance at the bank as well as with our third-party CBS / Switch vendors.

7.6 Sharing of information with Law Enforcing Agencies (LEAs): In terms of RBI guidelines, the bank has streamlined the process of data sharing between the bank and the Agencies, the bank has outlined a Standard Operating Procedure, in terms of procedural guidelines circulated by the Central Economic Intelligence Bureau, for implementation at the Bank. The SOP has been circulated to all branches and Head Office of the Bank for meticulous compliance.

7.7 Technology Vision Document: The Technology Vision Document aims at enhancing the cyber security posture of the Urban Co-operative banking sector against evolving IT and cyber threat environment through a five-pillared strategic approach GUARD, viz. Governance Oversight, Utile Technology investment, Appropriate Regulation and Supervision, Robust collaboration and developing necessary IT, Cuber security skills set. The bank has focussed on Board oversight over cyber security, IT vision document, Creation of reserve for implementation of IT/cyber security projects and ensure business availability.

8. Strengthening & augmenting Operational Resilience: Operational Resilience provides the ability to deliver critical functions in the event of any disruption. Disruptions may occur and the Bank shall be prepared to respond accordingly having measures in place to limit the impact. The Bank shall prepare itself to withstand, absorb, respond, adapt and recover and learn from disruptions with minimal impact on its critical operations. The Bank has enhanced/developed its operational resilience by ensuring business continuity, third-party risk management, ICT & Cyber Risk management, incident management, Security Operations Centre (SOC). Resilience has further been strengthened through audit processes such as concurrent, internal, revenue, information security, VAPT, system audit etc. besides subscribing to Anti-Phishing and Anti-Rogue applications.

9. Disclosures & reporting: The Bank may disclose relevant Operational Risk exposure information including significant operational loss events (if any) to its stakeholders, while not creating operational risk through such disclosure, to determine whether the Bank identifies, assesses, monitors and controls/mitigates Operational Risk effectively.

10. Lessons learned exercise and adaptation: The Bank shall conduct a Lessons Learned exercise, including root-cause analysis, after a disruption to a critical or important business service to enhance the Bank's capabilities to adapt and respond to future operational events. This also includes any potential material disruption to a third-party provider that feeds into the delivery of a critical business service. Further, the exercise shall define effective remediation measures to redress deficiencies and failure in the continuity of service. A report / self-assessment analysis document, post the incident containing the above shall be placed before the Board.

11. Continuous improvement through Feedback systems: The Bank shall promote an effective culture of learning and continuous improvement as operational resilience evolves through effective feedback systems. The Bank shall learn from its experiences as changes to its operational approaches or technology infrastructure mature over time.

12. Review: The Policy shall be reviewed by the Board annually or earlier, on receipt of fresh directives from the RBI.

****

Regd. Off.: C-2, First Floor, Wazirpur Indl. Area, Delhi-110052
+91-11-69340000-69340015
ipbank@ipbankonline.com
www.ipbankonline.com