UTI Pension Fund Ltd.

Risk Management policy

Version 2.2

Updated and reviewed in Board meeting held on 17.07.2026.

Index

1. RISK MANAGEMENT FRAMEWORK

BACKGROUND

As required by PFRDA, UTI Pension Fund needs to undertake an independent Risk Management Function, which will be responsible for identifying, evaluating, or measuring all inherent risk, as well as establishing controls to mitigate such risks.

The risks include:

Fund Management: Volatility in performance, style drift and portfolio concentration, interest rates movement.
Operations: Deal errors, settlement problems, NAV and fund pricing errors, inaccurate financial reporting.
Customer Service: Errors in deal processing, fraud etc.
Other Business Risks: Critical knowledge loss, Skill shortage, non-compliance, third party risks.

Board level Risk Management Committee of the UTI Pension Fund Ltd consisting of three Board Members, CEO, CIO, Chief Risk officer and Compliance Officer has also been constituted.

2. RISK MANAGEMENT POLICY

1. A risk register shall be maintained and periodically reviewed by the Risk Management Committee (RMC). Any additional/new risk that is identified shall be entered in the Risk Register and the same will be brought to the notice of RMC for its perusal in the next meeting. Risk registers shall be reviewed once in six months. The additional risk mitigation measures identified during the course of review should be implemented in a time-bound manner.

2. Preparation of an operational manual, containing the organization structure, objectives, job description for the various activities and reporting framework along with the internal controls and risk management framework.

3. The rights and obligations in respect of outsourced activities shall be clearly

laid down in the respective agreements, including the indemnity and confidentiality clauses.

4. In order to ensure effective internal control mechanism, as far as possible the general categories of duties of authorization, execution, custody, record keeping and reconciliation should be segregated.

5. The Risk Management Committee should review the process for permitting the use of new instruments or strategies (reviewed by Investment Management Committee) and ensure that appropriate risk management framework and policies are in place in respect thereof. Policies for initiating new activities should be consistent with the risk and return goals as well as the strategy and expertise.

6. The Risk Management Policy recognizes that UTI-PF is prone to external as well as internal Risk. As regards, external risks, the RM Policy stipulates that there shall be a Business Continuity Plan, duly approved by the Risk Management Committee, to ensure timely resumption of the interrupted business operations due to any natural disaster, unforeseen event or systems failure.

7. As regards internal risks, the Annexure -1 mentions various indicative risks and their control frame-work under following categories:
   (a) Fund Management
   (b) Operations
   (c) Sales, Marketing and Distribution
   (d) Customer Service
   (e) Disaster Recovery & Business Contingency
   (f) Other business risks.

3. REVIEW OF RISK MANAGEMENT FUNCTION

I Board of Directors

A Board Level Committee of UTI PF shall provide the overall guidance on Risk Management function, including –

(a) Setting the risk profile of the organization;
(b) Review of the Risk Management Policy and its implementation; and
(c) Review the Fund's approach to risk management and approve the key elements of its processes and procedures.

The Board has constituted a Risk Management Committee consisting of three Directors, CEO, CIO, CRO and Compliance Officer. The Committee shall meet at least on half-yearly basis.

II Chief Executive Officer (CEO)

The responsibility for implementation of Risk Management policy is delegated by the Board of Directors of UTI PF to the CEO. CEO shall ensure that the following documents, duly approved by the Board of Directors of UTI PF, are in place and the same are reviewed annually:

- Investment Policy, including Risk Philosophy
- Operating Procedures
- Compliance Manual
- Code of Conduct
- Disaster Recovery and Business Contingency Plan
- HR Policy
- IT and IT Security
- Scope of Internal Audit

4. RISK REPORTING

Risk reporting will be used to enhance risk communication across the organization. These reports will not only communicate the risk of individual schemes, but also provide inputs to fund management in their day to day fund management activity.

Further, the Risk management team shall reserve the right to independently conduct check / audits of the internal functions for implementing adequate internal controls and safeguarding the interests of the Company.

In addition to the information as may be called for by the Board, Chairman and RMC from time to time, the following reports shall be presented to the Risk Management Committee (RMC) of executives:

1. Status on implementation of risk management framework as approved by the Board;
2. Monthly risk Analysis Reports, covering the following main areas:

    i. Risk Adjusted performance measures such as Sharpe Ratio, Treynor Ratio and Sortino ratio in respect of Scheme portfolio vs. Benchmark Portfolio,
    ii. Analysis of Debt Portfolio in terms of movements Ratings, maturity profile and industry weights, and
    iii. Analysis of the movements in the assets allocation at portfolio level;

    A summary report shall be presented to the Chairman.

3. Quarterly reports on Critical observations in the Audit reports, including observations on non-compliance/deviations to the Risk Management Policy.
4. Summary of risks identified, existing control framework and proposed risk mitigation measures.
5. New activities being undertaken, along with the complete risk assessment and control framework.

5. CONTROL FRAMEWORK

Risk Area/Nature of Risks	Control Framework
i) Funds Management - Higher volatility in performance as compared to broad market, - Lower returns as compared to benchmark/peer group - Style drift and portfolio concentration, - Interest rate movements, - Liquidity Risk, - Credit risk - Delisting of Securities - Breach of Investment limits	1. Updated Investment Manual, covering, among others, the investment guidelines, investment decision making and recording process, delegation of powers and Review mechanism. 2. To adhere to the policies and procedures prescribed by the Board/Risk Management committee / Investment Committee 3. To measure performance on Daily/Weekly basis, as compared to benchmark and peer group 4. Regular review of portfolio, performance and exceptions by CIO, Investment Committee, Chairman and Board (including its Committees) 5. Investment Management Committee of Board should review and recommend action, if any, in respect of the following: a. Quarterly performance of NPS Schemes managed by UTI PF b. Periodic Portfolio review c. New investments during the quarter under review d. Credit rating review e. Compliance with the investment guidelines of PFRDA / NPS Trust and internal Investment Prudential Norms f. Distribution of Broker business within the specified limit 6. To have qualified and experienced Fund managers, research analysts and dealers with adequate experience in the industry. They shall be provided continuous training to understand the new products, markets and sectors. 7. To establish clear guidelines for best execution of investment deals, so as to avoid execution at sup-optimal prices. 8. Independent verification procedures for all deals should be established. Rates and prices shall be obtained from independent source. 9. Quarterly Review of illiquid securities and continuous review of exit options being given by the issuer companies for delisting of securities. 10. Updation of networth & paidup share capital of investee company in the mPower system on quarterly basis or as & when investee company publishes the figures related to Networth & paidup share capital. 11. Review & monitoring of investment limits through system. 12. Communication of alerts to Investment Team in respect of the investment limits for which 95% of the available limit has been utilized.

Risk Area/Nature of Risks	Control Framework
ii) OPERATIONS **Nature of Risks** - Errors in execution of investment deals, - Settlement problems, - NAV and fund pricing errors, - Inaccurate financial reporting, - Fraud, - Failure of mission critical systems and infrastructure, obsolete systems	▪ UTI PF shall buy insurance cover against third party losses arising from errors and omissions. Third party liabilities refer to liabilities arising out of financial loss to investors or any other third party, incurred due to errors and omissions of directors, officers, employees, R&T agents, etc. The level and type of cover should be determined by the Board. ▪ Operating procedures should lay down reconciliation activities and their frequency: • End-of-day broker confirmations with records of deals • End-of-day reconciliation of transactions with custodian data • At least once a week complete reconciliation of fund accounting system records with custodian records • Daily reconciliation between UTI PF and others (banks, counter party, etc). ▪ UTI PF shall establish a personal trading policy and a code of conduct for employees. ▪ Documentation of all NAV procedures and methodologies, including all elements critical to NAV calculations ▪ Concurrent Audit of the NAV and Dealing Function ▪ Audit of all financial reporting by internal and external auditors. ▪ UTI PF shall consider implementing integrated front and back office systems which will facilitate: ▪ Straight-through processing to allow one-time capture of trade details ▪ Pre-trade compliance checking ▪ Automatic time-stamping of deals ▪ Maker-checker authorizations ▪ In-built checks and controls ▪ Exception reporting ▪ Generation of deal confirmations ▪ Monitoring of outstanding confirmations, settlements and payments ▪ Cash management ▪ Access controls and firewalls, virus protection and other security functionality such as locking of trade data ▪ Integrated reporting. 8. UTI PF should ensure that the fund accounting systems used facilitate: • Validation of NAV calculations • Automated and manual price feeds • Identification of missing prices • Flagging of price variances beyond pre-established tolerance levels.

Risk Area/Nature of Risks	Control Framework
iii) IT Risk: Vulnerabilities in IT infrastructure	Vulnerability Assessment is carried out on half yearly basis & Penetration Testing on quarterly frequency. Observations found during this exercise are categorized as Critical, High & Medium. Based on the category tag, observations need to be resolved as per the below timelines: • Critical – 7 days • High – 15 days • Medium – 30 days After the points are closed the IT team requests for a re-scanning for the observed points to confirm the closure status of those points.
iv) Other Business Risks - Critical knowledge loss, - Attrition - Skills shortage, - Non-compliance, - Third party risks - Counterparty Risk	1. Well documented HR policies and procedures, addressing issues such as attracting and retaining key skilled staff, succession planning and career development plan. Appropriate incentive systems may also be established. 2. Ensure alternate staff availability in every function/ department to ensure uninterrupted & seamless continuity of functional activities. 3. Employment contract contains 3 months notice period which the employee is required to serve before his services terminate. This enables the HR department to arrange for suitable replacements & facilitate smooth transition. 4. Each department head shall be responsible for appropriate training and development of alternate staff in critical/key activities 5. Training plan for employees to update their existing skills and equip them with new skills. 6. A written contract of employment shall be entered into with the selected employees, covering among others compliance to internal and external regulations, confidentiality of information and observation of integrity and objectivity. 7. UTI PF shall have well laid down specific and measurable Organizational and Departmental Goals, Unambiguous instructions, priorities and Action Plan.

Risk Area/Nature of Risks	Control Framework
	8. The use and access rights of important/sensitive assets/data/information should be appropriately monitored and controlled. 9. The systems shall incorporate appropriate checks and balances, either to avoid errors due to accident/ignorance or to ensure early detection. 10. Potential acts of malicious nature should be avoided through use of 'preventive vigilance' 11. UTI PF should take appropriate Insurance policy to cover the damages caused by the employees actions. 12. UTI PF shall anticipate and respond well to changes of a market or regulatory nature that impact its reputation in the marketplace. 13. Establishment of a process to ensure continuous adherence to the Code of Ethics, Staff Rules and Code of Conduct under SEBI Regulations and / or PFRDA Guidelines / Regulations or other Acts / Rules / Regulations as may be applicable. 14. Policy On Prevention Of Self-Dealing, Front Running And Insider Trading of UTI PF shall be applicable. 15. Effective Performance Appraisal and Incentive system that – a. Facilitates achievement of the Organisation objectives and Mission b. Promotes identification of the early warning and initiation of the appropriate response c. Promotes effective utilization of the technology for improvement of the overall process 16. UTI PF and its officers shall follow the applicable Statutory Acts, Rules and Regulations in letter and spirit, concerning the areas being attended by the respective officers. *17.* As far as possible, the regulatory limits and restrictions should be incorporated in the systems *[to avoid any instance of regulatory violation].* 18. UTI PF shall implement and follow best business management practices and Good Corporate Governance. 19. As in case of other business risks, 'Scenario Analysis' exercise would help in anticipating and preparing for the changes in the regulatory environment. 20. UTI PF should have an effective and regular contact with the regulator(s). UTI PF should carry out due diligence of third party service providers before selection. The service level agreements (SLA) should prohibit the misuse of client information.

6. RISK APPETITE STATEMENT (RAS)

UTIPLF adopts a moderate risk appetite, recognizing that certain operational, technological, and strategic risks are necessary to achieve its business objectives. However, the organization maintains low tolerance for risks that could result in:

- Non-compliance with PFRDA regulations and statutory requirements.
- Financial fraud, data breaches, or cybersecurity incidents.
- Breach of subscriber confidentiality or compromise of personal data.
- Significant disruption to critical pension services.
- Reputational damage affecting stakeholder confidence.

Risks assessed as High (15–19) or Very High (20–25) on the Risk Heatmap shall require immediate management attention, documented mitigation plans, assignment of risk owners, and periodic reporting to the Risk Management Committee (RMC). Risks rated Medium (6–14) shall be managed through appropriate controls and regular monitoring, while Low (1–5) risks may be accepted with routine oversight unless circumstances change.

Risk Score	Risk Rating	Risk Appetite
1–4	Low	Acceptable – Monitor
5–14	Medium	Tolerable with Controls
15–25	High	Outside Appetite – Mitigation Required

7. RISK HEATMAP

Impact Scale	5	10	15	20	25
	4	8	12	16	20
	3	6	9	12	15
	2	4	6	8	10
	1	2	3	4	5
	Likelihood Scale (Probability of occurrence in a given year)				

Risk Score = Impact X Likelihood

UTIPLF approach to risk assessment is structured and dynamic in accordance with the principles outlined by the PFRDA guidelines.

1. Dynamic Risk Evaluation

Risk parameters such as consequence, likelihood, and overall risk level are inherently dynamic and subject to change based on: Regulatory updates from PFRDA, Operational events and service disruptions External environmental or technological shifts Therefore, fixed ratings are not prescribed within this policy. Instead, risk scores are determined contextually using the best available data and expert judgment.

2. Governance and Oversight

To ensure robust governance: A Risk Management Committee (RMC) at the Board level shall oversee the risk framework. Risk scores and assessments shall be compiled and reported to the RMC on a quarterly basis. The RMC shall review trends, emerging risks, and mitigation effectiveness, and may recommend strategic adjustments.

3. Compliance with PFRDA Guidelines

The organization ensures compliance with: PFRDA's operational and service standards for PoPs. Risk mitigation protocols including fraud prevention, cybersecurity, and business continuity as outlined in PFRDA Circulars Subscriber grievance redressal and SLA adherence as mandated by PFRDA regulations

Probability Matrix

Likelihood	1 – Rare	2 – Unlikely	3 – Possible	4 – Likely	5 – Almost Certain
Occurrence / Frequency	Once or twice in 10 years	Few times in 5 years	Few times a year	Few times a month	Continues or All the time
Probability	Conceivable, but only in extreme circumstances	Hasn't happened yet but could happen	Could happen and has occurred here or elsewhere	Could easily happen	Happens often

Impact Matrix

Impact Areas	1 – Insignificant	2 - Minor	3 – Moderate	4 – Major	5 – Catastrophic
Financial – Profitability	Less than 1% impact on PAT	1% to 2% impact on PAT	2% to 5% impact on PAT	5% to 8% impact on PAT	Greater than 8% impact on PAT
People	Loss of single staff	Loss of few staff	Loss of individual specialist personnel	Loss of key specialist team	Loss of one / several key executives
			Inability to attract talent over 6 months	Minor impact employee morale	Major impact on employee morale
				Inability to attract talent over 1 year	
Legal & Regulatory	Minor warning (Above Rs. 50,000)	Minor penalties (From Rs. 50,000 to Rs 5 lakh)	Major penalties (above Rs 5 lakh)	Major penalties and prosecution	Business suspension/ closure
Reputation / Corporate Image	Letter to local industry and press	Series of letters to local industry and press	Extensive negative local industry /social media coverage and short-term (3-6 months) disruption to customer confidence	Short term negative media coverage and disruption to client / investor confidence	Extensive negative media coverage and long-term disruption of client / investor confidence

8. Risk Control Self-Assessment RCSA - (PFM Side Risk)

Risk register
Date of Review: 16th July 2026
Reviewed By: Risk Officer & CRO

A. Statutory Compliance (PFM)

No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Risk Mitigation Measures	Responsible Officer
1.	**Regulatory & Compliance Risk** Non Adherence to various applicable statutes viz. PFRDA Regulations/ Income Tax Act/ Shops & Establishments Act etc., Profession Tax Act, Companies Act.	Un timely action by Back office persons/ Company Secretary etc.	1. Periodic Review by Internal Auditor. 2. Periodic Review by NPS Trust Board & PFRDA. 3. Compliance Manual covering IMA, PFRDA guidelines, CRA, Companies Act and Taxation laws has been documented 4. Valuation prices are received from the third-party valuer as appointed by PFRDA. 5. NAV movement on daily basis compared with previous day and index 6. Concurrent Audit of schemes 7. Statutory Audit & Detailed Audit by Independent Auditors appointed by NPS Trust	The timelines for the monthly, quarterly and Half yearly and Annual Compliances set by PFRDA is within 10 days from the end of each quarter. To mitigate the non compliance risk, the internal timelines have been set to 5 days from the end of each quarter in the Operations manual, which will ensure that same is submitted within the prescribed timelines.	For 1,2,3 and 7: CEO, CFO and CS & CRO. For 4, 5,6 : CFO

B. Fund Management: (PFM)

S. No.	What can happen (Effect)	How it can happen (Cause)	Existing Management Framework	Additional Risk Mitigation Measures	*Responsible Officer*
1.	**Regulatory & Compliance Risk** Non-adherence to the various Asset allocation limits, as per the Regulation/ Investment Management Agreement/ Investment Manual	Investment transaction not in line with the prescribed limits.	1. Daily Exception Report 2. Quarterly report on Investment Operations to the Board of UTI Pension Fund Limited & NPS Trust/ PFRDA. 3. Continuous review and management of schemes' portfolio by Fund Manager/ CIO 4. Periodic Review by Internal Audit, CEO and Risk Management Committee (Board) 5. Periodic review of exceptions thereto by CEO. 6. Updation of networth & paid up capital of investee companies in the mPower system on a quarterly basis or as & when investee company publishes the figures related to Networth & paidup share capital.	1. In future depending on the size of AUM, the Company would explore the possibility of implementing front office System with all in-built pre-trade system controls, duly integrated with back office system. Any additional risk mitigation measures will be implemented on case to case basis.	For 1, 2, 3, 5 & 6: CIO For 4 : CRO & CS

S. No.	What can happen (Effect)	How it can happen (Cause)	Existing Management Framework	Risk Mitigation Measures	*Responsible Officer*
2.	**Investment Risk** High volatility in performance of fund. Under performance of fund relative to Benchmark/ Peers.	High volatility of the underlying security/ Frequent change in investment style	1. Quarterly Report to the Board of UTI-PF & NPS Trust/ PFRDA on the performance of the schemes. 2. Periodic presentation on performance and Investment Strategy to the Board 3. Measurement of performance of fund as compared to that of peers/benchmarks on the past quarter, six-month, one year and since inception.	-	CIO
3.	**Investment Risk** Credit Risk / Counterparty Risk	Subscription to High-risk assets/Deterioration of the quality of the issuer.	1. For investment in debt instruments of companies with credit rating below 'AAA' but with credit rating of AA and above (i.e. the minimum acceptable rating is AA), approval of Executive Investment Committee is required. 2. Review of Credit ratings by Fund Manager/CIO. 3. Prudential Norms for investment in debt instruments. 4. All investments in Real Estate Companies, SPVs and Unlisted Companies with the approval of Investment Committee	-	CIO

S. No.	What can happen (Effect)	How it can happen (Cause)	Existing Management Framework	Additional Risk Mitigation Measures	*Responsible Officer*
4.	**Regulatory & Compliance Risk** Fraud Personal trading, insider trading & Front-running	Inappropriate Control over the investment process	1. Staff Rules 2. Regular Declarations from the FM/ CIO/ CEO in line with SEBI/ PFRDA regulations/Staff rules. 3. Restricted Access to Dealing room 4. Password controls in all critical databases 5. Recorded lines for all dealing operations 6. Prevention of Insider Trading	Fund Managers and Dealers shall, during market hours as applicable, ensure that their communication over telephone device is recorded to ensure a verifiable record of trades and interactions and shall be reviewed by the Internal Auditor. Fund Managers and Dealers will not swap the recording enabled SIM into any other device and will use the office provided with mobile phones and SIM together. In case the device is faulty, it should be immediately reported to Admin team for replacement with alternate device. Dealers and/or Fund Managers working out of the dealing room shall not access the personal mobile phones during the market hours. In exceptional cases, with the permission of CRO / RO, mobile phones/other communication device can be used during working hours outside the dealing room for personal emergencies with suitable records in the register. Mobile access register (maintained for recording usage of personal mobile phones by dealers and fund manager during market hours) shall be reviewed by the Internal Auditor. IT Team shall ensure that backup for all recorded modes of communication is adequately maintained for a period of 3 years. Further, the insider trading policy has also been implemented by the Pension Fund, in line with the PFRDA Guidelines.	CEO/ CRO

C. Back Office (PFM)

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
1.	**<u>Operational Risk</u>**				
(a)	Wrong valuation of unlisted/thinly traded equity securities	Wrong valuation provided by CRISIL.	- Investments are restricted to Top 200 companies in terms of Market Capitalization; which ensures enough liquidity. - Investment made via Public Offer is valued at the cost price until it is listed on National Stock Exchange or Bombay Stock Exchange.		CFO
(b)	Wrong valuation of Debt Securities	Wrong valuation provided by CRISIL.	- The valuation is done by CRISIL, a third party appointed by NPS Trust / PFRDA		
(c)	Valuation of securities	Details of new securities not provided to CRISIL.	- Security – wise valuation of previous day is compared with the valuation of present day. In addition, concurrent audit is done on daily basis.	-	

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
2	**Operational Risk** Wrong income accrual / valuation	Securities features wrongly defined in the system Corporate Action not factored / not intimated/ Wrongly factored by the CRISIL	1. Checking by an officer 2. Cross verification with NSDL listing 3. Concurrent Audit 4. Receipt of e-mail from CRISIL daily; 5. Cross – checked by the internal support system and ensured that Corporate Actions have been duly incorporated in the Valuation Files	-	CFO
3.	**Operational Risk** Erroneous Expenses accrual	Wrong accrual of AMC fees, other revenue expenses (not in line with PFRDA/Intern al guidelines)	1. Updation of the Master File based on approval of competent authority 2. Monthly review of actual expenditure vis-à-vis fund accruals 3. System control 4. Concurrent Audit	Concurrent Audit	CFO
4.	**Operational Risk** Outdated / inaccurate Valuation Policies	Non-updation of Valuation policies/metho dologies	1. Need-based review by the PFRDA	-	CFO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
5.	**Operational Risk** Delay in updation of NAV	Delay in receipt of information from various sources Systemic problems	1. Proper control mechanism through check-list and escalation systems on receipt of information 2. Availability of requisite IT support- staff	-	CFO
6.	**Operational Risk** Mismatch between Dealers record & Brokers contract Note	Inaccurate details by our dealers/Wrong Contract Notes	Exception Reports are generated and only confirmed deals are taken for NAV Computations	-	CFO
7.	**Operational Risk** Inaccurate Financial Reporting	Inadequate disclosure of the financial statement & non-adherence to PFRDA regulation/Inte rnal guidelines	1. Statuary Audit (of Half yearly/Annual Statements published) 2. Internal Audit 3. System controls, policies & procedures Manual, reviewed on periodic basis.	-	CFO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
8.	**Operational Risk** Idle Funds in Bank Account as per our books vis-a- vis Banks	Inaccurate Accounting	Daily Bank Reconciliation	-	CIO / CFO
9.	**Operational Risk** Non- Accuracy in payment of Bank charges/custo dy charges	Wrong rates/ Nos. of transactions	Checking of the bills to verify the rates as per the Agreement Custodian Charges with the approval of NPS Trust / PFRDA	-	CFO
10.	**Operational Risk** Non Adherence to internal rules and regulations	1. Absence of Reference Manual 2. Inadequate Control and Monitoring	1. Detailed Policy and procedure Manual, accessible to all officers and reviewed on annual basis. 2. Delegation of Powers in respect of Investments 3. Internal Audit 4. Delegation of powers for expenditure		CEO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
11.	**Operational Risk** Data Integrity Non-availability of critical systems / documents due to fire, natural disaster and other contingencies	Absence of business contingencies plan	1. Detailed IT policy of UTI PF is in place. 2. Storage of daily back-ups of database. 3. Storage of scanned copy of important documents in a common drive, which is backed – up by IT cell on daily basis. 4. Approved BCP	DR Drill is conducted on half-yearly basis.	CISO/ CTO CRO to conduct BCP / DR Drill
12	**Operational Risk** Wrong calculation / accrual of management fees / revenues	1. Change in AMC fees rate 2. Untimely action by Back office persons 3. AUM is incorrect	1. PFRDA direction 2. Quarterly approval of PFRDA / NPS Trust for AMC Fees 3. AUM figures obtained from Support system. The AUM is verified by NPS Trust / PFRDA from NSDL – CRA 5. Daily checking of accruals of AMC fees and other revenues	------	CFO
13.	**Operational Risk** Error in accounting of investment income	1.Non / wrong accounting of dividend 4. / interest income	1. Interest received on investments is verified extensively. 2. Investment income reinvested 3. Investments are redeemed whenever payments are to be made to vendors / creditors or other dues. 4. The profit / loss is booked on quarterly basis. 4. Investment ledger is tallied with register	----	CFO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	Responsible Officer
14.	**Operational Risk** Error in Accounting of Fixed Assets and Depreciation Over / under statement of fixed assets Inaccurate income	Non provision of adequate depreciation Classification under wrong account head	1. Asset wise details are maintained in Tally 2. Complete details of depreciation and book value of individual assets are recorded in Tally 3. Before updating the register, the bills are checked thoroughly 4. Physical verification of assets on yearly basis by DOA of UTIPF.	------	CFO
15	**Operational Risk** Discrepancy in vendor payments Excess expenditure / payments (Risk of recovery) Observation by Statutory and Internal Auditors Misrepresentati on of allowable / disallowable expenditure for income tax	1. Double payment 2. Payment without adequate approvals / support documents 3. Incorrect accounting	1. The bills are scrutinized thoroughly to avoid the disallowance of expenditure 2. The payments are released on the actual receipt of original bills 3. Before releasing any payment to vendor, the GL is checked to avoid double payment	-----	CFO
16	**Operational Risk** Inaccurate Financial Statements	1. Absence of well laid down policies and procedure or non – adherence thereof 2. Wrong classificatio n / allocation / capitalizatio n / accrual of various expenses 3. Non adherence to all applicable laws / accounting standards 4. Non – availability of all support documents	1. Policy and procedures approved by the Board 2. Quarterly review and analysis of the Trial Balance 3. Internal Audit on quarterly basis and external review / audit on quarterly / annual basis Co – ordination and follow – up with the respective department for expenditure settlements of the bills and creation / reversal of necessary provisions.	------	CFO

D. Other Risk (PFM)

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	Responsible Officer
1	**Business Risk:** Revenue declines due to reduced AUM inflows	Market volatility, poor fund performance	Diversified product offerings, marketing campaigns, client retention programs	Strategic partnerships, digital acquisition channels, performance-linked incentives	CEO / CIO
2	**Settlement Risk:** Counterparty failure to deliver securities	Counterparty insolvency, operational error, system failure	Approved counterparty list, settlement monitoring, margin requirements	Real-time settlement tracking, counterparty credit scoring, contingency arrangements	CIO / Dealers (Equity/ Debt)
3	**Liquidity Risk:** Inability to liquidate assets in stressed markets Mismatch between inflows and redemption requirements	Sudden redemption surge, poor forecasting	Cash flow monitoring, buffer reserves	staggered redemption structures	CIO / CFO
4	**Outsourcing risk:** Failure of outsourced services	Vendor negligence, SLA breach, lack of oversight	Vendor due diligence, SLAs, periodic audits	Exit strategies, multi-vendor fallback	Departmental Head/ CEO/ CS/ CRO
5	**IT & Cyber Risk:** Cyberattack on portfolio management systems System outage during trading hours	Malware, phishing, system vulnerabilities	Firewalls, encryption, access controls, regular audits,	employee cyber awareness training. All VAPT audit and system audit observations are reported by CISO/ CTO to ICSRM committee, ICSMR committee ensure critical observations of high category are addressed, ensure mitigation measure are taken in	CISO/CTO/ CRO

				timely manner and reported to RMC of board on quarterly basis.	
6	**People Risk:** Loss of Key Management Person Resignation & Inadequate succession planning	Retirement, resignation, health issues	Succession planning, leadership development, retention programs	board-level oversight, emergency delegation protocols	HR/ CEO

8. Risk Control Self-Assessment RCSA - (POP Side Risk)

Risk register
Date of Review: 16th July 2026
Reviewed By: Risk Officer & CRO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
1	**Operational Risk :** Incorrect subscriber onboarding data (KYC errors, wrong details)	Manual entry errors, lack of training	Maker-checker process, KYC validation tools	Regular staff training, automated KYC checks	RM/ RH/ POP Head Operation / CEO
2	**Operational Risk :** Delays in contribution remittance to Trustee Bank/CRA	System downtime, manual delays	TAT monitoring and defined workflows	Backup systems, escalation matrix	POP Head Operation / CEO
3	**Operational Risk :** Mis-selling – Providing misleading or incomplete NPS information	Lack of understanding of the product / disregard to the internal processes/ wrongful conduct for achieving targets	Details escalation process is established in malpractice matrix. Sales scripts, audit trails	Surprise checks of suspicious transactions	CEO / POP Head Operation/ CRO/ CS/ CO (PoP)
4	**Operational Risk :** Fraud – Misappropriation of subscriber contributions	Insider threat, weak controls	Segregation of duties, audit logs	Whistleblower policy Internal Audit & surprise checks of suspicious transactions	CEO / POP Head Operation/ CRO/ CS/ CO (PoP)
5	**Regulatory & Compliance Risk :** Breach of PFRDA SLAs for service requests	Delays, system inefficiencies	SLA dashboards, periodic reviews	SLA-linked KPIs, automated alerts	CEO / POP Head Operation/ CRO/ CS/ CO (PoP)
6	**Regulatory & Compliance Risk :** Non-compliance with AML/CFT guidelines	Poor monitoring, lack of awareness	Compliance training	Enhanced due diligence, periodic audits	POP Head / CO (PoP) Breaches, if any, will be reported to the CRO / CS / Ceo by the above mentioned personnel.

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
7	**Financial Risk :** Loss of revenue due to PFRDA fee revision	Regulatory changes	Financial forecasting, buffer reserves	Diversify revenue streams	CEO & CFO
8	**Financial Risk:** Penalties for wrong processing or breach of TAT	Human error, system bugs	Quality checks, SOPs	Error-proofing tools, staff accountability	RM / RH / POP Head Operation / CEO
9	**Technology Risk:** CRA system integration failure	API issues, poor testing	Pre-launch testing, fallback systems	Redundant systems, vendor SLAs	CISO / CTO/ CTDO
10	**Technology Risk:** Adoption of new technology	Resistance, lack of training	Change management policy	Pilot testing, user training programs	CISO / CTO/CEO
11	**Cybersecurity Risk :** Cyberattack or data breach (subscriber data theft)	Phishing, weak passwords	Firewalls, encryption, audits	Regular penetration testing, employee awareness programs. All VAPT audit and system audit observations are reported by CISO/ CTO to ICSRM committee, ICSMR committee ensure critical observations of high category are addressed, ensure mitigation measure are taken in timely manner and reported to RMC of board on quarterly basis	CISO /CTO

S. No	What can happen (Effect)	How it can happen (Cause)	Existing Control Framework	Additional Risk Mitigation Measures	*Responsible Officer*
12	**Infrastructure Risk :** System downtime during critical cut-offs	Power failure, hardware issues	UPS, DR site	Cloud migration, real-time monitoring	CISO /CTO
13	**Reputational Risk :** Negative publicity due to fraud, mis-selling, or poor service	Fraud, poor service	PR protocols, grievance redressal	Proactive communication, service quality audits	All employees of UTIPFL
14	**People Risk:** High staff attrition impacting service	Low morale, poor pay	HR policies, exit interviews	Career development plans, retention bonuses	HR / CEO
15	**Business Continuity Risk:** Voluntary PoP branch closure or closure of branches due to disaster/pandemic	Natural disaster, pandemic	BCP policy, remote access	Alternate PoP locations, remote onboarding tools	CEO

9. Version Details

Version	Approval Date	Reviewed / Amended
1.	18th July 2025	Reviewed.
2.	17th October 2025	Updated & reviewed.
2.1	20th January 2026	Updated & reviewed.
2.2	17th July 2026	Updated & reviewed.