Aditya Birla Sun Life
Pension Fund Management Ltd.

ADITYA BIRLA CAPITAL
PENSION FUND

ADITYA BIRLA SUN LIFE PENSION FUND MANAGEMENT LIMITED

RISK MANAGEMENT POLICY

Version 5.2

Correspondence & Registered office:
Aditya Birla Sun Life Pension Fund Management Limited
(Formerly known as Aditya Birla Sun Life Pension Management Limited)
One World Center, Tower 1, 16th Floor,
Jupiter Mill Compound, 841, Senapati Bapat Marg,
Elphinstone Road, Mumbai, Maharashtra - 400 013

Tel: +91 22 6723 9203 / 04 | care.pensionfunds@adityabirlacapital.com
https://pensionfund.adityabirlacapital.com
CIN: U66000MH2015PLC260801

Document Version Control

Version	Owner of the Document	Date of Approval by RMC	Date of Approval by Board	Revised Policy Effective from	Nature of Change
1.0	Risk & Compliance	27/07/2016	27/07/2016	27/07/2016	New Policy
1.1	Risk & Compliance	24/10/2017	24/10/2017	24/10/2017	Revised
1.2	Risk & Compliance	14/01/2019	14/01/2019	14/01/2019	No change
1.3	Risk & Compliance	23/04/2019	23/04/2019	23/04/2019	Formatting changes
1.4	Risk & Compliance	18/10/2019	18/10/2019	18/10/2019	Change in frequency of review Introduction of alternate arrangement for the offices of key Officials of the Company
1.5	Risk & Compliance	20/07/2021	20/07/2021	20/07/2021	Included the Stress Test to Monitor Short Term Risk of Investment Portfolios'
2.0	Risk Management	18/04/2024	18/04/2024	18/04/2024	Re-structuring
2.1	Risk Management	19/07/2024	19/07/2024	19/07/2024	Re-structuring
3.0	Risk Management	22/10/2024	22/10/2024	22/10/2024	Addition of fraud risk in risk categorisation as per the Anti-Fraud Policy.

3.1	Risk & Compliance	23/01/2025	23/01/2025	23/01/2025	No change
3.2	Risk & Compliance	17/04/2025	17/04/2025	17/04/2025	No change
4.1	Risk & Compliance	18/07/2025	18/07/2025	18/07/2025	Change in Risk Mitigation measure under Investment Risk category from two successive downgrades to case-to-case basis.
4.2	Risk & Compliance	17/10/2025	17/10/2025	17/10/2025	No change
4.3	Risk & Compliance	16/01/2026	16/01/2026	16/01/2026	No change
5.0	Risk & Compliance	17/04/2026	17/04/2026	17/04/2026	Changes to Section 3.2 pertaining to Business Impact Analysis
5.1	Risk & Compliance	17/07/2026	17/07/2026	17/07/2026	Review
5.2	Risk & Compliance	16/10/2026	16/10/2026	16/10/2026	Review

Table of Contents

Policy Objective: 5
Corporate Risk Philosophy: 6
Risk culture: 6
Creating and Implementing an ERM framework: 8
Mandate and Commitment: 8
Designing an ERM Framework: 9
Implementing an ERM Framework: 9
Monitoring and review of the framework: 9
Continual Improvement of framework 9
Roles and responsibilities in an ERM framework: 9
ERM Framework Structure: 10
The phased approach of ERM: 11
Critical Success Factors: 11
Risk management framework review and approval: 11
Annexure A: Enterprise Risk Management framework – Process and Procedures: 11
Annexure B: Risk Category Definition 12
Annexure C: COSO Framework 14
Business Continuity Plan:` 17

Preamble:

Aditya Birla Sun Life Pension Management Limited (ABSLPFML) is engaged in the business of investment management of the pension corpus received from NPS Trust and regulated by the Pension Fund Regulatory and Development Authority (PFRDA).

In terms of the Investment Management Agreement (IMA) entered into with the NPS Trust, the Company is required to have a Risk Management Policy duly approved by the Board of Directors.

Policy Objective:

The objective of this document is to formulate the Risk Management Framework in Company, which will help to govern the risk identification, assessment, measurement and reporting process of all risks. The documents aim to ensure that all material risks can be identified and managed in a timely and structured manner.

Business managers make decisions every day about which risks to accept and which to avoid leading to Risk Management on daily basis. An Risk Management framework helps to build a structured process that ensures all material risks are identified and understood by senior management.

Objective of ERM framework:

The Objective of building a Risk Management (ERM) framework is to facilitate business management in:

- **Understand and manage risks and not eliminate risks**

The objective of ERM is to manage risks. In any environment (especially a dynamic business requirement), risks cannot be avoided or eliminated. They can only be managed efficiently and on a timely basis and ERM aims to achieve the same.

- **Aligning risk appetite and strategy**

Business risks cannot be identified and managed in isolation of the risk appetite and the business strategy. Risk appetite is the combined levels of overall business risks that a company is willing to take. In other words, risk appetite is the level of aggregate risks that the company can undertake and successfully manage over an extended period of time. Business strategy is the operating plan that the business has developed for the forthcoming years.

- **Enhancing risk response decisions**

ERM aims to have a consolidated risk database, which facilitates a speedy risk response thus supporting the functions in case the risk manifests.

← Reducing operational surprises and losses

An effective ERM framework can assist business management to reduce the operational surprises and losses by framing mitigation strategy for key business risks so that the same can be implemented in a timely and efficient manner

← Seizing new business opportunities

ERM facilitates business management to evaluate new opportunities as a risk mitigation technique. Through ERM, the management can evaluate new business proposal and products. For example, a risk management strategy to diversify business share would be evaluating and carrying research on new products across industry.

← Improving deployment of capital

Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

Enterprise Risk Management Framework:

Corporate Risk Philosophy:

In conducting its business activities, company is driven by shareholder and policyholder expectations, external ratings and its positioning in the marketplace, will take on those risks that meet the objectives of the organization. Risk management should be aligned with the corporate vision and strategy, and needs to be embedded within the overall business management practices.

The Risk management approach is being developed by taking into account the organizations overall governance, management, reporting process, policies, philosophy, culture & regulatory architecture.

Company has in place Operational Risk Management Framework that supports excellence in business processes, systems including Business Continuity & Disaster Recovery framework to ensure resumption of time sensitive activities within defined timeframe at defined levels. One of the risk mitigation strategy for managing operational risk that company has includes ensuring at all point of time to have adequate insurance cover for all resources including assets.

Risk culture:

Risk Management is most effective when employees at all levels of an organization share a common philosophy and set of principles regarding risk. The Company's risk culture has to be determined and demonstrated from the top, must be clearly articulated, and must align with the company's strategic vision, its core values, and other elements of corporate culture if they are to enhance organizational effectiveness.

Risk management enhances shareholder value. The company can more effectively compete and win through superior execution of the risk management function throughout all levels of the organization.

To ensure that the company achieves and maintains a strong risk culture, every employee must feel accountable for achieving the best results for his or her business unit and for the company as a whole.

Business decisions are made at all levels of the organization, and every employee has a role in identifying exposures, communicating concerns, and escalating risk issues as appropriate.

The following fundamental principles are required in an effective risk management program:

► Acting with Integrity

Acting with integrity is one of Company's core values, and goes hand-in-hand with effective risk management. This means that we make the right decisions for the right reasons, even when it is difficult to do so or may mean the loss of business.

► Customer Alignment

The company accepts risk from and shares risks with customers. This requires that the company proactively and clearly communicate to customers the nature of the risks that are being shared. It also means that the company must fully understand the risks it has acquired from customers, and understand the value of the management of those risks on behalf of the customer.

► Discipline

This requires discipline through the development of sound business practices, attention to established processes, a clear delineation of accountabilities, and adherence to company policies. Discipline is also achieved through commitment to a strong control environment to forge an appropriate balance between stewardship and entrepreneurship

► Embedding Risk Management

Effective risk management requires that risk management be embedded into the business so that individuals making business decisions do so with full awareness of the risks inherent in the products or activities being managed or considered. In order to make appropriate risk/reward tradeoffs, we must ensure that we have the capability throughout the organization to undertake rigorous, unbiased identification and assessment of risk. Investment must be made in risk management infrastructure to support this effort.

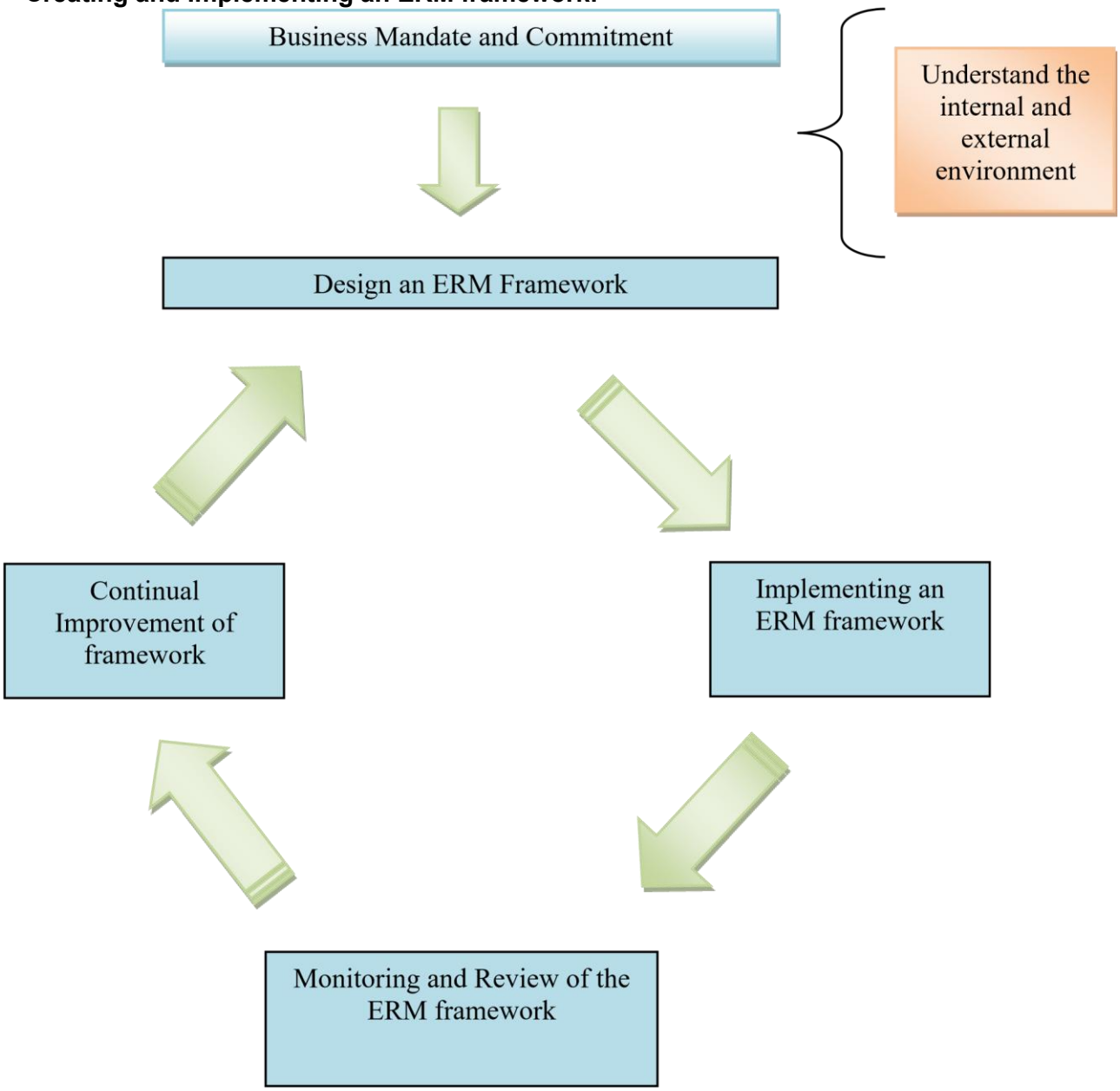
► Promotion of Full and Transparent Communication

Effective risk management is a cross-disciplinary exercise involving employees throughout the organization that relies upon clear channels of communication -- up, down and across the organization. Emerging risk issues must be escalated to the appropriate levels of senior management. Transparency in our risk management program requires that we are able to communicate the risk profile of the organization to our stakeholders.

► Collaboration

Collaboration creates value – that the whole is greater than the sum of its parts – and strives to share and leverage our tools, processes and experience across the organization.

Creating and Implementing an ERM framework:



Mandate and Commitment:

Management should:
- Articulate and endorse the risk management policy
- Communicate the benefit of risk management to all stakeholders
- Ensure that necessary resources are allocated to risk management

Designing an ERM Framework:

- Understand the organization and its environment
- Clear the framework objectives
- Integrate into organizational processes
- Specify accountability and resources
- Establish internal/external communication and reporting mechanisms.

Implementing an ERM Framework:

- Developing a plan for implementation
- Implementing the framework (phased approach mentioned below)

Monitoring and review of the framework:

- Periodically measure progress against risk management plan
- Continuous review of the framework
- Review effectiveness of risk management process.

Continual Improvement of framework

- Based on the review of the framework, the framework should be updated to make the organizational risk management process more robust.

Roles and responsibilities in an ERM framework:

Everyone in an entity has responsibility towards risk management.

► The Chief Executive Officer is ultimately responsible and would assume ownership for an effective risk management framework.

► Leadership team members and Functional Heads usually have key support responsibilities in managing the overall ERM framework by guiding the risk management team in carrying out the ERM framework.

► The Risk management team is responsible to support the management in implementing the overall ERM framework.

► Functional managers support the entity's risk management philosophy, promote compliance with its risk appetite, and manage risks within their spheres of responsibility consistent with risk appetite.

► Other entity personnel are responsible for executing enterprise risk management in accordance with established directives and protocols.

► The Risk Management Committee provides important oversight to enterprise risk management, and is aware of and concurs with the entity's risk appetite. The Risk Management Committee composition and charter has been separately listed.

► A number of external parties, such as customers, vendors, business partners, external auditors, regulators, and financial analysts often provide information useful in effecting enterprise risk management, but they are not responsible for the effectiveness of, nor are they a part of, the entity's enterprise risk management.

► Internal Audit will review the risk management practices within the department on a regular basis and report as appropriate on issues arising from these reviews.

► All employees will actively support and contribute to risk management initiatives and maintain an awareness of risks (current and potential) that relate to their area of responsibility

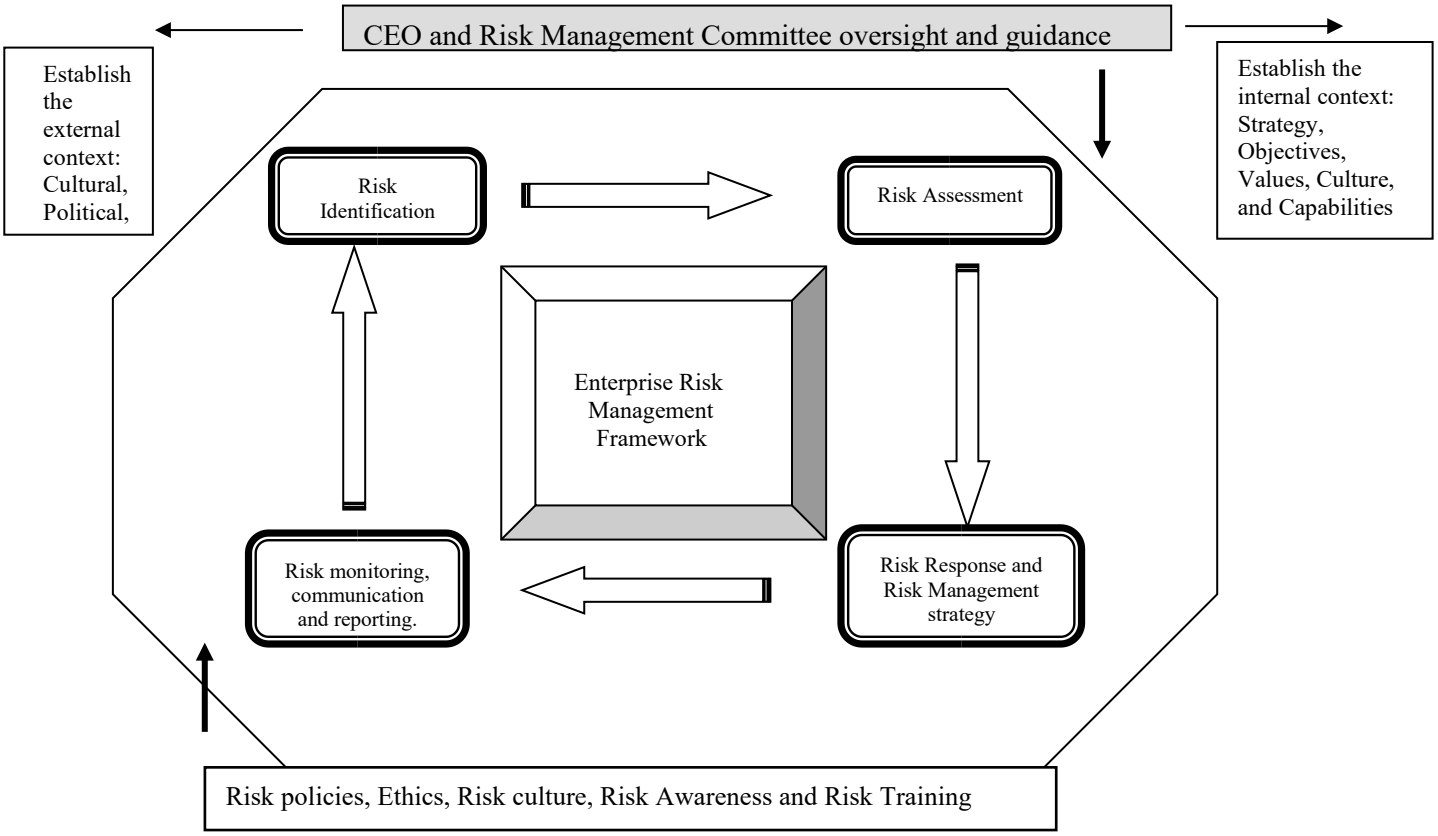
ERM Framework Structure:

ERM framework at Company is in line with the phased approach proposed by COSO (Committee of Sponsoring Organisation), which has provided guidance on developing models on integrated risk management. The risk management framework as designed by COSO will be integrated with the ERM framework in Company apart from the best practices for the risk management in the industry. The four phases are listed as follows:

← Risk identification;
← Risk Assessment;
← Risk Response and Risk Management strategy; and
← Risk monitoring, communication and reporting.

All the phases would be jointly required to be carried on by the functional heads and the risk management team. The Risk Management Committee would closely monitor the overall process. ERM is not a one-time project but an ongoing practice. All the above phases are to be operative on a continuous basis. Other critical elements such as Risk Review Committee oversight, efficient risk management policies, risk management committee charter etc also play an important part in the overall ERM framework.

The phased approach of ERM:



Critical Success Factors:

- Senior Management Commitment in implementation of the Risk Management framework
- Complete support from Functional heads and risk champions in implementation of the framework
- Free access to records, information and personnel throughout Company in order to identify and address potential risk management issues
- Authority to carry out its mandate and to follow up on issues identified and recommendations made related to the critical business risks.

Risk management framework review and approval:

The risk management team will review the risk management framework on an annual basis.

Annexure A: Enterprise Risk Management framework – Process and Procedures:

Risk Management framework

The Company has an Enterprise Risk Management (ERM) framework covering procedures to identify, assess and mitigate the key business risks. Aligned with the business planning process, the ERM framework covers all business risks including reputation risk, operational risks, regulatory risks, insurance risks, people risks and market risks.

Below are key points of framework:

► Risk Management team conducts an exercise annually for identification of key business risks and relevant mitigation strategies
► The functional RSCAs and the internal audit reports will also govern the risk framework for Company.
► Identified risks would be suitably categorized
► Identification of Key Risk Parameters and Key Risk Drivers
► Key risk metrics would then be presented to the Risk Management Committee
► Risk Management will seek periodical status updates for all Top business risks as identified and review the risk metric as well.
► The key risk updates will be quarterly updated to the Risk Management Committee

Annexure B: Risk Category Definition

In order to facilitate discussions and identification of risks and exposures, the matrix of risk categories have been developed. Utilization of common risk categories and an understanding of the sources and consequences of risk events will allow for consistency in reporting, facilitation of aggregation and contribute to the enterprise risk management framework.

In addition, we need to understand all of the potential aspects of risks, which will help in risk assessment. In order to provide a framework for that understanding, we have developed a matrix of risk categorization, which is structured as follows:

- **Risks Drivers**
  In order to manage risk effectively, risks need to be specifically defined so that appropriate action plans can be developed. This section provides further breakdown of risks within the main categories.

- **Source**
  This column identifies the key activities, which create an exposure to the company within the specific risk categories.

- **Exposure Triggers**
  Exposure triggers are the actual events that need to occur before a risk manifests itself into a situation that requires specific management actions and impacts the organization.

- **Direct Consequences**
  Consequences are both financial and non-financial impacts to the organization as a result of a risk event.

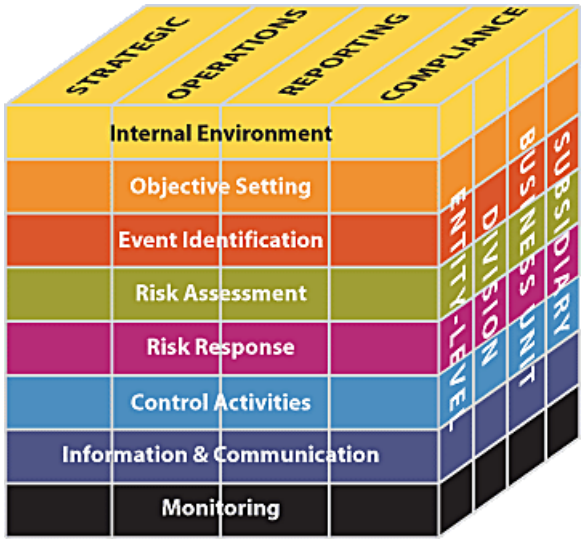
Annexure B (A): Risk Categorisation

Risk Category	Key Risk	Key Risk Driver	Risk Mitigation Measures
Investment Risk	1. Market Risk 2. Credit Risk 3. Fund Management Risk	➢ Interest Rate movement ➢ Rating downgrade ➢ Underperformance of Fund	➢ Through Duration of the fund. ➢ ~~After two successive downgrades~~ On case to case basis & evaluate internally. ➢ Monitoring of Monthly Performance ➢ Monitoring of Risk-Adjusted Return Ratios
Cyber Security Risk	1. Access right risk 2. Information Security risk 3. DR site management risk 4. Application downtime Performance Issue 5. System Failure risk	➢ Unauthorized access to the system and application ➢ Lack in DR site management periodically ➢ Computer virus and non-availability of sufficient backup for critical data	➢ Ensuring the system and process are immune from viruses and sufficient back up is obtained of the critical and sensitive Company's data. ➢ Periodical System Audit ➢ Periodical DR Testing
Operational Risk	1. Process risk 2. NAV error 3. Fund Settlement 4. People Risk	➢ Absence of defined SOP ➢ Inadequate System Automation ➢ Shortage of Security / Overdraft ➢ Employee Attrition	➢ Ensuring all the critical operational SOPs are up to date vis –a –vis the process. ➢ Automation of critical processes ➢ Ensure key employee back-up
Regulatory Risk	1. Reporting Error 2. Non-Compliance 3. Change in regulation	➢ failure to adhere any regulatory requirement ➢ Mismanagement of reporting due dates	➢ To ensure that the reports are thoroughly worked out and are audited / reviewed periodically. ➢ Efficient tracking the changes in the regulatory

			environment and circular issued by the Concerned Authorities.
Fraud Risk	1. Subscribers/Claimant Fraud 2. Intermediary / Entity Fraud 3. Internal Fraud 4. Digital Fraud	➢ Inadequate/weak verification process ➢ Lack of awareness and training ➢ Weak internal controls ➢ Inadequate segregation of duties ➢ Lack of cybersecurity awareness ➢ Weak authentication protocols	➢ Provide timely training and awareness sessions to all employees ➢ Ensure all potential frauds reported are assessed timely as process defined in the Anti-Fraud policy.

Annexure C: COSO Framework

COSO (Committee of Sponsoring organisations) Framework



COSO is an International voluntary private organisation dedicating to improve the quality of financial reporting through corporate governance, business ethics and effective internal control. The COSO framework talks about an eight-step approach towards building an effective enterprise risk management strategy. The eight-step approach is spread over the entire departments on an organization to meet the overall strategic, operations, reporting and compliance requirement of an organization.

Annexure C – (a) - Methodology for Risk Assessment as per RCSA

Risk Measure as per RCSA

Risks have been rated in terms of probability and impact. The scale is defined as under:

Probability of Occurrence	Weight (A)	Impact on Occurrence	Weight (B)	Risk Measure(A*B=C)
0-6 Months	5	Very High	5	1 to 5 – Low Risk
6 months - 2 years	4	High	4	6 to 15 – Medium risk
2-5 years	3	Moderate	3	16 – 25 – High Risk
5-10 years	2	Low	2	
10 & above	1	Minimal	1	

Control Measure Scale as per RCSA

Automation	Maker/Checker	Frequency	Preventive/Reactive	Score
A	Y	S	P	25
A	Y	S	R	24
A	Y	E	P	23
A	Y	E	R	22
M	Y	S	P	21
M	Y	S	R	20
A	N	S	P	19
A	N	S	R	18
M	Y	E	P	17
M	Y	E	R	16
A	N	E	P	15
A	N	E	R	14
M	N	S	P	13
M	N	S	R	12
M	N	E	P	11
M	N	E	R	10
No Control				0

Level of Automation	Manual (M)	Automated (A)
Maker/Checker Control	Yes (Y)	No (N)
Frequency of Control	Event Based (E)	Set Frequency (S)
Preventive/Reactive	Prevntive (P)	Reactive (R)

Annexure D: Stress Test of Investment Portfolio

The Short-Term volatility in the market adversely impact the performance of the fund. In case of equity fund, the short-term movement of the benchmark index is highly co-related to the sentiment of the market whereas the actual equity portfolio is built keeping in the long-term strategy to create wealth. Similarly, in case of debt fund, the short-term movement of the interest rate impact the overall term structure of the yield curve, because the movement of the interest rate sometime happens on the shorter end of the yield curve and sometimes it happens on the longer end of the yield curve. In both ways, the actual performance of the debt funds gets impacted.

To measure such type of the Short-Term Risk, a suitable stress test scenario is required to be implemented and monitored on every quarter-end so that the Risk Management Committee and Board will be apprised about the potential risk under such circumstances and the likely drop in the value of the portfolio in terms of Mark-To-Market losses.

The Format to measure the Stress Test: -

Name of the Portfolio	Initial Market Value	Equity Market Fall 5%		Equity Market Fall 10%		Equity Market Fall 20%	
		Final Market Value	MTM Loss	Final Market Value	MTM Loss	Final Market Value	MTM Loss
E1							
E2							

Name of the Portfolio	Initial Market Value	Yield Curve Move up 50 bps		Yield Curve Move up 100 bps		Yield Curve Move up 200 bps	
		Final Market Value	MTM Loss	Final Market Value	MTM Loss	Final Market Value	MTM Loss
G1							
G2							

Name of the Portfolio	Initial Market Value	Yield Curve Move up 50 bps		Yield Curve Move up 100 bps		Yield Curve Move up 200 bps	
		Final Market Value	MTM Loss	Final Market Value	MTM Loss	Final Market Value	MTM Loss
C1							
C2							

Business Continuity Plan:

Table of Contents

1.0 Background: 18
2.0 Business Continuity Planning Objectives: 19
2.1 Scope: 19
2.2 Assumptions: 19
2.3 Limitations & Exclusions: 20
3.0 Requirements.....20
3.1 Risk Assessment: 20
3.3 BCP/DR Plans: 21
3.4 Testing: 21
3.5 Change Management: 22
3.6 Contact List / Call Tree: 22
3.7 Annual Certification: 22
3.9 Incident Reporting: 23
4.0 Training & Awareness: 23
5.0 Critical Service Provider/Vendor Requirements: 23
6.0 Waivers / Exception: 23
7.0 Provision of Resources 24
7.1 Competency 24
7.2 Roles & Responsibilities 24
7.3 Outsourcing: 25
8.0 Internal Audits: 25
9.0 Review: 26
Appendix A 26

1.0 Background:

Companies face myriad risks from threats such as natural disasters, operational breakdowns, hostile political situations, employee malevolence, and damage to critical information technology and telecommunications systems etc. These threats can result in lost profits, injuries, loss of life, damage to a company's reputation, or, in extreme cases, the demise of the organization.

Business Continuity Planning is the ability and readiness to manage business interruptions in order to provide continuity of services at a minimum acceptable level and to safeguard the financial and competitive position in the short and the longer term. Companies that develop and maintain Business Continuity Plan ('BCP' or 'the plan'), reap enormous benefits such as improved levels of safety, marketplace advantages, enhanced reputation for reliability and most important of all, the maximum potential to resume their business operations in the event of a disaster.

Aditya Birla Sun Life Pension Fund Management Limited ('ABSLPFML') actively supports the development and implementation of a comprehensive BCP focusing on the timely recovery of critical business processes and information technology systems at the Head Office at One India bulls Centre.

2.0 Business Continuity Planning Objectives:

1. Ensuring a proactive response to any contingency

2. Protecting the safety of ABSLPFML Employees & Visitors
3. Ensuring Recovery of identified Critical activities within an agreed timeframe; and
4. Ensuring that we adhere to our Client, Contractual, Legal & Regulatory requirements.

Policy statement

To have a planned response in the event of any contingency ensuring recovery of critical activities at agreed levels within agreed timeframe thereby complying with various regulatory requirements and minimizing the potential business impact to ABSLPFML. Additionally, to create a system that fosters continuous improvement of business continuity management.

Scope:

The scope of the policy covers recovering critical business processes as identified in the Business Impact Analysis in the event of any one of the contingency impacting Operations at One India bulls centre but not limited to only the following specific disaster scenarios:

- Earthquake;
- Fire;
- Bomb Blast;
- Floods;
- Terrorism and civil unrest;
- Information Technology failure; and
- Any other scenario as identified in the Annual Risk Assessment process.

Assumptions:

The assumptions are:

- The probability of a disaster impacting the entire country is remote and not taken into consideration while preparing the plan; and
- The mobility of the Emergency Response Team & Individual Function Recovery Team personnel is not impacted due to any State/Government directive surpassing the Logistic Support Team's action plan.

Limitations & Exclusions:

The Risks accepted by ABSLPFML Management during the Annual Risk Assessment exercise are not covered as a part of this Policy.

3.0 Requirements

3.1 Risk Assessment

Risk Assessment is the process of identifying the risks that can adversely affect an organization and its facilities during a time of disruption or disaster. Risk assessment at ABSLPFML is done **annually** and must identify organizational risks in the following areas i.e. environmental, facilities and technologies. The consolidated risk assessment report is prepared and signed off by Chief Finance Officer and Compliance Officer.

The components of a Risk Assessment are:

- Use of a standard methodology to determine the events and environmental conditions that can adversely affect the organization;
- Determination of the damage such events can cause, and the controls needed to prevent or minimize the potential loss;
- Identify the effectiveness of the Current Risk Management strategies in place; and
- Provision of a cost effective analysis to justify any additional mitigating controls to be put in place.

3.2 Evaluation of RTO & RPO for critical services

ABSLPFML shall adhere to all applicable regulatory requirements pertaining to business continuity, including the evaluation of RTO & RPO for critical services. The organization may, as deemed fit from time to time, undertake additional evaluation activities, such as BIA, to enhance the business continuity and resilience program.

The Business Impact Analysis (BIA) is the process of identifying financial and non-financial impact in the event a particular process is disrupted. It helps in assessing the functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure, and evaluating the cost for such controls. Once business functions are identified, the amount of time the business function can be interrupted must be determined. This will help in determining the Recovery Time Objective (RTO) for the processes the order of priority for re-establishment of the business function.

3.2.1 Recovery Rating:

Based on the RTO chosen by the Unit each process is assigned a Recovery rating. The rating structure is as per Appendix A.

3.3 BCP/DR Plans:

3.3.1 Business Continuity Plan:

The Business Continuity Plan will include all critical functions identified through the Business Impact Analysis. Each of the processes would have a Recovery Procedure to ensure that recovery happens within a stipulated timeframe as determined by the RTO (Recovery Time Objective). There would be

critical staff identified who would be recovering the critical business processes from an Alternate Site. The plan is reviewed annually & approved by Chief Finance Officer and Compliance Officer.
The Pandemic plan outlines the plan of Action in case of a Pandemic outbreak. The plan is reviewed annually & approved by Chief Finance Officer and Compliance Officer.

3.3.2 Disaster Recovery Plan:

IT Team maintains a Disaster Recovery Plan to recover all its Critical systems & applications in case of any Outage /incident s impacting the IT Infrastructure at our primary data centre. The plan is reviewed and approved annually

3.3.5 Alternate Site Plan:

ABSLPFML has an Alternate Site Recovery Plan to recover its critical Plans from an alternate site in case of a localized or Regional disaster. The plan is reviewed annually & approved by Chief Finance Officer and Compliance Officer.

3.4 Testing:

To ensure that plans and the Standard Operating procedures are viable & operational Business Continuity Plans and Disaster Recovery Plan are tested as per the Recovery Rating. Disaster Recovery tests will involve the recovery of appropriate systems applications and infrastructure to support the critical business functions.

3.4.1 Desk Check:

The objective of the exercise is to review the contents of the plan.

3.4.2. Table Top Simulation:

This is an Extended Desk Check exercise to check the interaction and the roles of the participants.

3.4.3 Operational:

This involves one or a sample of Functional Recovery team members moving to and recovering the process from an alternative site.

The Business Continuity, Disaster Recovery & Alternate Site would be tested annually. The functions/processes would be selected as per their criticality rating & frequency as defined in the table below:

Recovery Rating	Testing Methodology	Frequency
V1	Operational	Annually
V2	Operational	Annually
V3	Operational	Annually
V4	Operational	Annually
V5	Table Top Simulation	Once in Two Years
V6	Table Top Simulation	Once in Two Years

Besides this the following would be tested as per the frequency mentioned in the table below:

Activity	Frequency
Call Tree Testing	Annually
Evacuation Drill	Annually

3.5 Change Management:

1. All applicable changes pertaining to the organization, processes and technology must be reflected in the Business Impact Analysis in the annual revision cycle or as and when deemed necessary.

2. All system and application changes or new system implementations in the production environment must be made on the Disaster Recovery site depending on the criticality.

3.6 Contact List / Call Tree:

Contact List/Call Tree prepared need to be updated quarterly & tested annually.

3.7 Annual Certification:

Annual certification needs to be provided confirming the implementation and effectiveness of BSPM's Business Continuity Management System Framework. The Attestation is provided by Chief Finance Officer and Compliance Officer.

The overall objective is to have an up-to-date:

Business Impact Analysis of all business functions;

a. Business Continuity and Disaster Recovery Plans for all functions; and

b. Complete testing of the recovery process for all the business functions and applications.

3.8 Resource requirement:

Adequate resources in terms of funding and manpower will be allotted to Business Continuity Planning Team so that the requirements under this policy are met. Functional areas will allocate appropriate staff when required for maintenance of their Business Impact Analysis, Business Continuity Plan, training and testing's.

3.9 Incident Reporting:

All employees to report any untoward incident with a potential to disrupt normal operations at ABSLPFML on the Incident reporting ID i.e. Sandhya.upadhyay@adityabirlacapital.com & abslpm.riskmanagement@adityabirlacapital.com

4.0 Training & Awareness:

All employees should be aware of their roles and responsibilities under a BCP Scenario. The awareness training should be provided to all employees. BCP Team (Chief Finance Officer and Compliance Officer) to conduct training sessions for all Emergency Response Teams & Individual Function Recovery Team members through Mailers or Workshops or Screensaver or Risk Awareness Quiz.

5.0 Critical Service Provider/Vendor Requirements:

ABSLPFML Functions must ensure that any Critical Service Provider contracted to perform a service within ABSLPFML has Business Continuity and Disaster Recovery plans that support the functional recovery plan.

6.0 Waivers / Exception:

In case of technical or business reasons it is not possible to comply with this Standard, a waiver must be requested. The waiver needs to be approved by the Functional Head and Chief Finance Officer and Compliance Officer.

7.0 Provision of Resources:

7.1 Competency

The organization shall appoint a person with appropriate seniority and authority to be accountable for Business Continuity Planning policy implementation.

7.2 Roles & Responsibilities

7.2.1 Risk Management

The Chief Finance Officer and Compliance Officer are responsible for coordinating & managing the overall BCP program. Working with the functional areas and their service providers, the BCP Team (Chief Finance Officer and Compliance Officer) facilitates the program by:

1. Facilitating periodic Business Impact Analysis (BIA) discussions with the functional areas.
2. Document all changes to Business Continuity Plan documentation periodically.
3. Organize periodic Business Continuity Planning testing exercises.
4. Review the need for building evacuation and Business Continuity plans for branches.
5. Evaluate the adequacy and implementation of the Business Continuity Planning procedures at least on an annual basis.

7.2.2 Business Functional Areas

The functional areas identified as Critical as per the BIA are ultimately **owners** of their processes including the supporting applications and data. The functional areas identify their critical processes;

the vulnerabilities that threaten them and the planning required to keep them operational or recoverable in a timely manner.

1. Identified Functional area will designate an IFRT leader as the BCP contact. This person is the point of contact though functional heads are still the owners for their plans and processes.

2. Identified Functional areas will ensure that the recovery strategy is communicated to all employees within their function.

3. The respective Individual Function Recovery Team Leader & Emergency Response Team Leader shall intimate BCP Team (Chief Finance Officer and Compliance Officer) of any changes in the process, system & people for their team.
4. Identified Functional areas will keep Business Continuity planning in mind while developing any strategic plans or changes in business (so that recoverability is not affected).

5. The alternative arrangement for the office of the officers are as under:

Officers	Alternative arrangement
CEO and Principal Officer	Any Director or Principal officer appointed by the Board of Directors.
CFO & Operation Manager	Senior Manager- Operation
CIO	Fund Manager
Fund Manager	CIO

7.2.3 Business Support Functions:

IT is the custodian of the information technology systems in the company and is responsible for maintaining and testing the Disaster Recovery Plans for applications and systems for each critical function.

Administration function is responsible for the overall management & maintenance of the facility.

Risk Management & Internal Audit is responsible for auditing and reviewing Business Continuity program for compliance with this policy.

7.2.4 Employees

All Employees need to be aware of the Initial Response Team (IRT) and Personnel Support Team (PST) member on their floors. They need to be well versed with the Do's and Don'ts in any contingency the Assembly Point for their facility and communications sent by BCP Team (Chief Finance Officer and Compliance Officer) on a periodic basis.

7.3 Outsourcing:

All outsourcing contracts will include an annexure on vendor BCP preparedness that will have to be completed by vendors entering a contract for providing services.

8.0 Internal Audits:

All the functions supporting ABSLPFML's key products and services shall be subjected to an Internal Audit as per the defined frequency below:

Recovery Rating	Frequency
V1	Annually
V2	Annually
V3	Annually
V4	Annually
V5	Annually
V6	Annually

9.0 Review:

The Policy shall be reviewed at least quarterly or as and when significant changes occur within ABSLPFML or the environment in which it operates.

Appendix A

Recovery Rating	Definition	Minimum Business Continuity Strategy
V1	The business functions & applications are vital to successful business performance & must be restored to an acceptable level of capability within no more than 4 hours.	Formal Business Continuity Plans are required. Alternate Site Planning requires a pre designated recovery site where the function can be recovered. All the applications requiring local installation should be installed at the Alternate Site.
V2	The business functions & applications are essential to successful business performance & must be restored to an acceptable level of capability within no more than 24 hours.	Formal Business Continuity Plans are required. Alternate Site Planning requires a pre designated recovery site where the function can be recovered. All the applications requiring local installation should be installed at the Alternate Site.
V3	The business functions & applications are essential to the successful business performance & must be restored to an acceptable level of capability within no more than 48 hours.	Formal Business Continuity Plans are required. Alternate Site Planning requires a pre designated recovery site where the function can be recovered.
V4	The business functions & applications are essential to successful business performance & must be restored to an acceptable level of capability within no more than 72 hours.	Formal Business Continuity Plans are required. Alternate Site Planning requires a pre designated recovery site where the function can be recovered.

Recovery Rating	Definition	Minimum Business Continuity Strategy
V5	The business functions & applications are desirable for efficient business performance; however restoration may be delayed up to two weeks.	Formal Business Continuity Plans are required.
V6	The business functions & applications are not critical to successful business performance and restoration may be delayed for more than two weeks.	Formal Business Continuity Plans are required.