

Maharashtra State
Electricity Distribution
Company Limited

Risk Management
Policy

Terms & Definitions

- 1) ARR- **Aggregate Revenue Requirement** represents the total revenue a regulated entity (like an electricity distribution or transmission company) is allowed to recover from consumers during a specific financial year to cover its costs and earn an approved return.
- 2) CAIDI- **Customer Average Interruption Duration Index** measures the average duration of a sustained interruption experienced by customers who experience an interruption.
- 3) CCMP- **Cyber Crisis Management Plan** is a structured framework that defines how an organization prepares for, responds to, manages, and recovers from major cyber-security incidents that could disrupt operations, compromise data, or threaten critical infrastructure
- 4) CVSS- **Common Vulnerability Scoring System** is a standardized framework used to measure and communicate the severity of software vulnerabilities. It assigns a numerical score from 0.0 to 10.0, where higher scores indicate more severe vulnerabilities.
- 5) **High Risk Vendor** is a third-party supplier whose failure, misconduct, security weakness, financial instability, or non-compliance could cause significant operational, financial, legal, safety, cybersecurity, or reputational harm to the organization.
- 6) LTIFR - **Lost Time Injury Frequency Rate** measures the rate of injuries resulting in at least one full shift/day lost from work, excluding the day of injury.
- 7) MAIFI- **Momentary Average Interruption Frequency Index** measures the average number of momentary interruptions experienced by a customer during a specified period.
- 8) SAIDI- **System Average Interruption Duration Index** measures the average total duration of sustained interruptions experienced by a customer during a specified period.
- 9) SAIFI- **System Average Interruption Duration Index** measures the average number of sustained interruptions experienced by a customer during a specified period.
- 10) TRIFR - **Total Recordable Injury Frequency Rate** measures the rate of all recordable injuries occurring in a workforce relative to total hours worked.
- 11) VAPT- **Vulnerability Assessment & Penetration Testing**, a security exercise in which external or internal security professionals scan and test systems (applications, servers, network, Application Programming Interfaces (APIs), endpoints, cloud assets, etc.) to identify vulnerabilities that attackers could exploit.

1. Introduction

1.1. About MSEDCL

Maharashtra State Electricity Distribution Company Limited (MSEDCL), a wholly owned corporate entity CIN: U40109MH2005SGC153645 under the Maharashtra Government, was incorporated under the Companies Act on 31st May 2005 after restructuring the erstwhile Maharashtra State Electricity Board to distribute electricity from the end point of transmission to the end consumers. MSEDCL is a Public Company in the category of 'State Government Company' registered under the Companies Act 1956, with the main objectives of developing, operating and maintenance of distribution system for supplying electricity to the consumers in its area of supply. As a deemed distribution licensee under section 14 of the

Electricity Act 2003, MSEDCL is carrying out the supply of power to the end users as well as maintaining the wire business for supply of such power.

Currently, MSEDCL provides electricity throughout the State of Maharashtra and in few suburbs of Mumbai city and is one of the largest power distribution Company both in the country and in Asia, in terms of number of consumers and electricity supplied whereby it serves more than 3.2 Crores consumers with around 70,000+ employees.

1.2. Need of the Policy

MSEDCL acknowledges that, as a major power-distribution utility, it operates in an environment characterized by inherent uncertainties and volatility that can affect both its financial performance and non-financial outcomes. Given the scale of its infrastructure, the magnitude of its financial exposure, its responsibility for public safety, and its extensive regulatory obligations, a comprehensive Risk Management Policy is indispensable. Implementing a structured risk-management framework will enable MSEDCL to anticipate, mitigate, and respond to potential threats, thereby safeguarding stakeholder interests, enhancing confidence in achieving organisational objectives, and supporting sustainable business growth. It also complies with the statutory provisions under the Companies Act, 2013 and Rules made thereunder.

2. Objective of the Policy

The main objective of this policy is to ensure sustainable business growth with stability and to promote a proactive approach in identifying, evaluating, reporting and managing risks associated with the business. In order to achieve the key business objectives, the policy should establish a structured and disciplined approach to Risk Management, including the development of the Risk Register, in order to guide decisions on risk related issues.

The specific objectives of the Risk Management Policy are:

1. To identify risks and potential threats that may hinder the achievement of the organization's business objectives.
2. To continuously monitor and review the evolving risk landscape in response to internal business activities as well as external business, economic, and operating conditions.
3. To assess exposure to all categories of risk on a regular basis and reduce such exposure to the lowest level reasonably practicable or achievable.
4. To identify and periodically measure key risk indicators and initiate timely and appropriate actions to manage and minimize risk exposure.
5. To conduct regular reviews of key risk controls to ensure they remain relevant, resilient, and effective in addressing identified risks.

2.1. Scope and applicability

The policy guidelines are devised in the context of the future growth objectives, business profile envisaged and new business endeavours and the emerging global standards and best practices amongst comparable organization

This Risk Management Policy is applicable to the following under the jurisdiction of MSEDCL:

1. Corporate Office and all regional/zonal offices.
2. Circle offices, field offices, and liaison offices.
3. All operational assets, including substations, distribution lines, and customer service centres.
4. All project sites, whether under construction or investigation, within Maharashtra and any future locations outside the state.

3. Risk management approach

Risk Management at MSEDCL is a structured process designed to identify, assess, and address risks that may impact the organization's ability to achieve its objectives. This approach ensures that risks are managed proactively rather than reactively, enabling resilience and operational continuity.

Risk management is not confined to a single function, rather, it is the responsibility of every stakeholder within the organization, including the Board of Directors, Senior Management, and all MSEDCL personnel. It applies across all functions, departments, projects, and operational units, covering both strategic and day-to-day activities.

The primary objectives of establishing a Risk Management Process are to ensure that:

- **Comprehensive Risk Identification and Centralization**

All risks faced by the organization, i.e., operational, financial, regulatory, technological, or environmental shall be systematically identified and documented in a centralized risk repository. This enables top management to maintain a holistic view of the organization's risk exposure.

- **Continuous Risk Assessment and Mitigation**

Identified risks shall undergo structured assessment to determine their likelihood and impact. Appropriate mitigation strategies shall be developed and implemented, followed by monitoring and periodic reviews to ensure effectiveness and adaptability to changing conditions.

4. Contours of Risk Management Framework

Effective risk management within a power distribution utility begins with a structured and disciplined process of risk identification, followed by a logical and comprehensive risk categorization framework. Given the operational complexity, regulatory oversight, and public service obligations associated with electricity distribution, risks may originate from multiple sources, i.e., internal operations, sectoral dynamics, and broader external environments. Accordingly, the organisation adopts a proactive and systematic approach to identify potential events, conditions, and circumstances that may adversely affect operational reliability, financial sustainability, regulatory compliance, and service delivery.

This structured classification then forms the foundation for **Risk Assessment & Mitigation**, where risks are evaluated in terms of their likelihood and impact, prioritised accordingly, and addressed through appropriate control measures, governance mechanisms, and monitoring frameworks. Together, these processes ensure that risk management is not a standalone activity but a continuous, integrated cycle supporting operational resilience, regulatory compliance, and sustainable performance.

4.1. Risk Identification

The risk identification process is embedded across functional levels of the organisation and is carried out through periodic operational reviews, project monitoring mechanisms, audit observations, regulatory assessments, incident analyses, and stakeholder feedback. This enables early recognition of vulnerabilities in processes, systems, infrastructure, human resources, and commercial practices. Identified risks are documented, evaluated for their likelihood and impact, and subjected to appropriate mitigation planning through established control mechanisms and governance structures.

4.2. Risk Categorization

For effective assessment and management, risks are categorised into three principal groups. Unit Risks encompass internal risks arising from operational processes, systems, human resources, and infrastructure. Industry Risks relate to sector-specific factors, including regulatory changes, market dynamics, technological advancements, and competitive pressures. Macroeconomic Risks cover external influences such as economic conditions, policy developments, financial markets, and other broader environmental factors that may impact organisational performance.

1. Unit Risks – Internal Operational, Project, People & Commercial Risks

Unit Risks arise from within the organisation and are directly linked to how the utility manages its core business processes, infrastructure, human capital, systems, and commercial activities. These risks can undermine operational stability and service delivery if not proactively managed.

a. Operational Process & Technical Risks

- i. Operation & Maintenance (O&M) risks:** It reflects the organisation's ability to sustain day-to-day operations and preserve asset integrity while meeting performance, safety, and service obligations, particularly in relation to the operation and maintenance of the distribution network and associated operational, technical, and support systems.
- ii. Distribution network performance shortfalls:** Failure to maintain distribution assets (feeders, transformers, substations) can increase outage frequency and duration, affecting reliability and customer satisfaction. Legacy infrastructure and insufficient preventive maintenance elevate the risk of equipment failure.
- iii. Metering and data integrity issues:** Faulty or obsolete meters, manual readings, and metering inaccuracies contribute to poor consumption data and billing errors, potentially inflating non-technical losses.

- iv. **Power theft and unauthorised consumption:** Illegal connections, meter tampering, and energy diversion significantly increase commercial losses and complicate loss reduction efforts.

b. Project Execution & Contractual Risks

- i. **Errors in project estimation and scope definition:** Inadequate demand forecasting, network design gaps, and incomplete project specifications increase cost overruns and schedule delays.
- ii. **Project delivery delays:** Supplier and contractor under-performance or logistical bottlenecks in equipment procurement can delay key initiatives such as grid modernisation, feeder segregation, and automation roll-outs.
- iii. **Contractual ambiguity or unfavourable terms:** Weak contract safeguards and poorly defined performance KPIs expose the utility to disputes, cost escalations, and contractual non-conformance.

c. Commercial & Revenue Cycle Risks

- i. **Billing shortfalls:** The billing shortfalls occur upstream of revenue recovery. Electricity is supplied and consumed, but the corresponding revenue is partially billed, incorrectly billed, or not billed at all.
- ii. **Collection (recovery of dues) shortfalls:** High incidence of delayed or defaulted bill payments severely straining cash flows with increased receivables, bad debts & strain on operational obligations.
- iii. **High AT&C (Aggregate Technical & Commercial) losses:** Persistent technical losses due to network inefficiencies, and commercial losses due to theft and billing inefficiencies, directly undermine financial performance.
- iv. **Disputes and legal exposures:** Consumer grievances related to billing errors, tariff disputes, and service quality can escalate into prolonged litigation or regulatory appeals.

d. Human Resource & Safety Risks

- i. **Management risk:** It is the risk of adverse impact on organisational performance, governance, or continuity arising from deficiencies, instability, or failure of key managerial persons or leadership positions, including risks related to capability, succession, decision-making, and conduct.
 - ii. **Skill and competency gaps:** Shortages of specialised technical personnel, particularly for digital systems, automation, and advanced analytics, impede operational excellence.
 - iii. **Labour unrest and workforce safety:** Disruptions due to labour disputes or work stoppages can affect field operations, especially during peak demand or outage restoration periods.
- e. **Compliance risks:** Compliance risk refers to the potential for legal, financial, operational, or reputational consequences resulting from the organisation's failure to adhere to applicable

laws, regulations, regulatory directives, contractual obligations, and internal policies governing its operations, financial management, and governance.

- i. **Regulatory & Statutory:** It refers to the obligation of the organization to adhere to all applicable laws, statutes, rules, regulations, regulatory orders, and license conditions governing the electricity distribution business, as prescribed by central and state authorities and sector regulators.
- ii. **Operational & Technical Compliance:** It refers to the adherence to prescribed technical standards, operational codes, procedures, and performance norms governing the safe, reliable, and efficient operation of the power distribution network and consumer interface.
- iii. **Financial Compliance:** It is the risk arising from non-adherence to financial laws, accounting standards, regulatory financial directives, and funding-related obligations applicable to the DISCOM.

2. Industry Risks – Sector-Wide, Regulatory & Competitive Risks

Industry risks are associated with the structural and regulatory environment of the electricity distribution sector, including market dynamics, technology trends, and regulatory frameworks that impact all distribution utilities.

a. Regulatory & Policy Risks

- i. **Tariff determination uncertainty:** Delays or adverse decisions in tariff orders by the Maharashtra Electricity Regulatory Commission (MERC) can compress margins and constrain cost recovery. Independent bodies may face regulatory pressure, complicating timely tariff approvals.
- ii. **Policy volatility:** Frequent changes in industry rules, compliance requirements, and subsidy frameworks increase complexity in planning and revenue forecasting.

b. Competitive and Market Risks

- i. **Pressure from alternative service providers:** While most DISCOMs operate in monopoly markets, increasing interest in private participation (including franchisee arrangements in some regions) could alter service expectations and performance benchmarks.

c. Sector Transition & Technology Risks

- i. **Integration of distributed energy and renewables:** Growth in rooftop solar, EV charging, and distributed resources introduces variability and complexity in load management and network balancing.
- ii. **Digital transformation risk:** Adoption of advanced technologies (AMI, smart grid systems, outage management systems) poses project, interoperability, and cyber-security risks if not effectively governed.

d. Financial Risk Across the Sector

- i. **Persistent sector-wide financial stress:** Even after tariff adjustments, DISCOMs continue to operate with weak financial metrics due to costs exceeding revenues, delayed subsidy compensation, and accumulated debt.

3. Macroeconomic Risks – External Economic, Policy & Environmental Risks

Macroeconomic Risks reflect the influence of broader economic, fiscal, and environmental conditions that affect the power distribution sector's operating environment and financial resilience.

a. Economic & Financial Market Risks

- i. Macroeconomic slowdowns:** Economic downturns can depress industrial and commercial consumption, undermining revenue collections and cross-subsidy structures that support residential tariffs.
- ii. Financial risks:** It is the risk that refers to a possibility that an organization's financial health, performance, or stability could be negatively impacted by adverse changes in financial variables or structural weaknesses in its financial framework, potentially affecting its capacity to maintain operations, fulfil its obligations, and achieve its strategic goals.
 - a) Borrowing risks:** It refers to the possibility that the organisation may be unable to raise, refinance, service, or effectively manage its debt on acceptable terms and within required timelines, potentially constraining liquidity, increasing financing costs, or limiting financial flexibility.

Rising borrowing costs impair the utility's ability to fund capital investments and refinance existing debt.

b. Policy & Political Risks

- i. Subsidy and tariff issues:** State government decisions to mandate deeply subsidised or free power to specific consumer classes, without assured reimbursement, can create material cash flow deficits and escalate financial stress.
- ii. National reform initiatives:** Large-scale programs such as distribution sector bailouts or privatization proposals can introduce transition risk, requiring organisational adaptation and potential restructuring.

c. Environmental & Natural Hazard Risks

- i. Weather and climate impacts:** Severe weather events (unseasonal rains, storms) have caused extensive damage to distribution infrastructure, leading to significant restoration costs and operational disruptions.
- ii. Climate variability risk:** Long-term climate trends may alter peak load patterns and stress distribution networks beyond historical design norms.

4.3. Risk Assessment

Risk assessment is undertaken to systematically evaluate the potential impact of identified risks on the achievement of organisational objectives. This assessment considers both qualitative and quantitative factors to determine the extent to which risks may affect operational performance, financial stability, regulatory compliance, and strategic outcomes.

Each identified risk is evaluated based on its **potential impact** and **likelihood of occurrence**, using a structured assessment framework. Based on this evaluation, risks are categorised into **Low, Medium, or High**-risk levels to facilitate prioritisation and informed decision-making.

4.3.1. Key Risk Indicators (KRI)

The following KRIs have been adapted for MSEDCL. Thresholds are set annually and reviewed quarterly:

Risk Area	KRI	Typical Threshold / Target	Frequency	Risk Owner
Reliability	SAIDI (duration/customer); SAIFI (interruptions/customer); CAIDI (duration/interruption); MAIFI;	Annual improvement $\geq 10\%$	Monthly/ Quarterly	Distribution/ Operations
Reliability (Granular)	% Feeders exceeding SAIDI/SAIFI limits; Worst-circuit index;	Reduction in worst-circuit population $\geq 10\%$ YoY	Monthly/ Quarterly	Distribution/ Operations
Safety	TRIFR/LTIFR; Near-miss/ Incident reports for electrical divisions; Training completion %	Zero fatalities; Increasing reporting frequency; >90% mandatory training completion for technical staff	Quarterly	Human Resources/ Safety
Cyber/IT	Critical vulnerabilities unpatched; VAPT findings open; Mean Time to Detect/Contain; CCMP drill readiness	Critical vulnerabilities remediated <30 days; Incident containment within <24 hours; 2 CCMP drills/year	Quarterly	Information Technology
Financial	Operating cash days EBITDA margin % vs ARR/MYT	Cash days $\geq 45-60$ EBITDA margin within $\pm 100-150$ bps of	Monthly/ Quarterly	Finance

Risk Area	KRI	Typical Threshold / Target	Frequency	Risk Owner
	allowed Variance vs approved ARR (revenue & cost) DSO (Days Sales Outstanding) Working capital cycle (days) Debt maturity profile risk (≤12-month maturities ÷ total debt) Average cost of debt (trend) Refinancing coverage (committed lines/Mark to Market vs next-12-month maturities) Covenant breaches / waivers (count) Interest rate mix (fixed vs floating %)	approved trajectory ARR variance within ±3–5% DSO reducing ≥5 days/quarter Working Capital cycle improving Quarter-on-Quarter Near-term maturities ≤20–25% of total debt Avg. cost flat to down Quarter on Quarter (or ≤ policy band) Refinancing coverage ≥1.2× of next-12-month needs Zero covenant breaches Fixed-rate share ≥60–70% (policy-aligned)		
Commercial	AT&C loss %;	AT&C loss reduction ≥1–2% points/year;	Monthly/ Quarterly	Commercial

Risk Area	KRI	Typical Threshold / Target	Frequency	Risk Owner
	Billing efficiency %; Meter data validation success %; Collection efficiency %; Overdue receivables >90 days (% of total); Legal/recovery case disposal rate;	Billing Efficiency ≥ 98–99% overall ≥97%– 99% Collection Efficiency ≥ 98–99% overall with ≥97% in high-risk segments; >90-day over-dues <15% of receivables; Case disposal ≥90% within Service Level Agreements (SLAs);		
Operation & Maintenance (O&M)	Feeder/DT failure rates (per 100 km / per 100 DT) Preventive maintenance compliance % (plan vs actual) Mean Time to Repair (MTTR) Critical spares availability %	Failure rates reducing ≥5% in existing levels Preventive maintenance compliance = 100% MTTR compliance as per SOP Critical spares availability ≥90%	Monthly/ Quarterly	Operations
Supply Chain	% Procurements from Trusted Sources; % Vendors with cyber clauses;	>95% trusted procurement; Contracts with cyber clauses / total critical vendors;	Quarterly	Procurement Procurement + Legal

Risk Area	KRI	Typical Threshold / Target	Frequency	Risk Owner
	Audit completion %;	100% high-risk vendors audited;		Internal Audit
Projects	Distribution Projects progress vs plan;	Schedule variance <10%;	Quarterly	Projects
	Capex absorption %;	Capex absorption ≥90%		Finance + Projects
	Defect density	Defects per module/site experiencing continuous reduction trend		Projects
Compliance	Timeliness & accuracy of regulatory financial submissions (ARR/MYT, true-up, audited Financial Statements)	100% on-time submissions & Zero material restatements;	Quarterly	Tariff Regulatory Cell
	# Regulatory notices/penalties;	100% timely publication of reliability indices;		-do-
	Subsidy claim–receipt reconciliation gap (₹ & days)	Subsidy gap ≤30 days; reconciliation zero-difference monthly		
	Audit opinion quality (no. of qualifications)	No audit qualifications (or action plan ≤ 90 days for each)		Commercial
	Audit findings closure rate	Closure within agreed timelines		Respective Business/ Function Heads

Risk Area	KRI	Typical Threshold / Target	Frequency	Risk Owner
Management/ Managerial	Succession coverage for critical roles (% positions with named successors)	Succession coverage ≥90%	Quarterly	Human Resources
	Leadership vacancy days (critical roles)	Vacancy ≤45 days per critical role		
	Leadership churn (rolling 12-month %)	Churn ≤10% (12-month)		
	Mandatory governance & training completion %	Training completion ≥95%		

4.4. Risk Mitigation Plan

For risks assessed as material, appropriate **risk mitigation strategies** are formulated and implemented. These strategies include clearly defined action plans, ownership, and timelines, with the objective of reducing the probability of occurrence and/or minimising potential disruption to operations and business continuity.

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
Unit Risk	Operational Process & Technical Risks	Operation & Maintenance risks	• Transition from reactive to preventive and predictive maintenance practices • Use asset health assessments to prioritize maintenance and replacement of high-risk assets • Strengthen maintenance planning and execution through system-driven scheduling and monitoring • Ensure availability of critical spares and skilled manpower to minimize outage durations • Reinforce safety, reliability, and performance through audits, training, and root-cause analysis
		Distribution network performance shortfalls	<u>Infrastructure Modernisation</u> • Accelerate SCADA integration and distribution automation leveraging AI/ML partnerships • Prioritise critical feeder reinforcement and transformer capacity upgrades through risk-based planning <u>Performance Monitoring</u> • Deploy real-time network health dashboards for voltage profile monitoring & feeder loading • Comply with Service Level Agreements (SLAs) for feeder fault restoration with escalation pathways <u>Operational Resilience</u> • Implement Feeder redundancy planning (alternate supply paths) to shorten outage durations
	Metering and data integrity issues		<u>Smart Meter Rollout</u> • Fast-track AMI deployment with network communications resilience <u>Meter Quality & Calibration</u> • Lifecycle management for meter replacement with third-party calibration audits

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
			<u>Data Governance</u> Establish formal data quality frameworks, detecting reading anomalies and reconciliation loops
		Power theft and unauthorised consumption	- Deploy DT-feeder energy audits and big data analytics to identify irregular patterns - Hotlines and rapid response teams to detect and disconnect unauthorized connections - Awareness campaigns about penalties under the Indian Electricity Act.
	Project Execution & Contractual Risks	Errors in project estimation and scope definition	- Emphasis on central project estimation unit with historical build cost database - Mandate independent technical and commercial review before approval - Adopt digital cost-estimation tools aligned to evolving MERC norms
		Project delivery delays	- Implement Project Management Office (PMO) with milestone tracking and SLAs for key partners - Utilize digital workflow tools for change requests and approval turnaround times
		Contractual ambiguity or unfavourable terms	- Standardise bid documents and enforce pre-award legal vetting - Assign responsibility matrices clearly between MSEDCL and contractors
	Commercial & Revenue Cycle Risks	Billing and collection (recovery of dues) shortfalls	- Ensure tight integration of billing, reconciliation, and collection streams - Prepaid metering pilots in high-risk regions. - Digital payment reminders and segmentation-based collection strategies - Adopt consumer-wise differentiated recovery strategies based on risk profiles and payment behaviour - Implement time-bound arrear settlement schemes/procedures for legacy receivables, where appropriate - Deploy legal and enforcement measures selectively for chronic defaulters, within regulatory norms

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
		High AT&C (Aggregate Technical & Commercial) losses	• Feeder-level accounting and performance-linked incentives for loss reduction. • Targeted infrastructure upgrades in high-loss pockets.
		Disputes and legal exposures	• Strengthen Tariff Regulatory Cell to handle tariff and compliance disputes • Standardised dispute escalation and mediation clauses in vendor agreements
	Human Resource & Safety Risks	Management risks	• Maintain formal succession and continuity plans for all critical managerial and technical positions • Define clear roles, responsibilities, and delegation of authority to reduce dependency on individuals • Strengthen leadership capability through targeted training in regulatory, financial, and operational areas • Monitor leadership vacancies and transitions to prevent control or decision-making gaps • Reinforce governance and ethical standards through oversight, reviews, and accountability mechanisms
		Skill and competency gaps	• Structured training tied to technology upgrades • Certifications aligned with safety and technical excellence • E-learning modules /Training hours tied to performance appraisals.
		Labour unrest and workforce safety	• Safe workplace frameworks aligned with legal standards • Protective protocols and police support in high-risk assignments • Workforce engagement forums to address grievances
	Compliance Risks	Regulatory & Statutory	• Maintain a centralised regulatory compliance register covering all applicable statutes, MERC regulations, tariff orders, license conditions, and government directives • Establish a regulatory compliance calendar with clearly defined responsibilities, timelines, and escalation protocols

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
			• Implement structured internal reviews to ensure adherence to tariff orders, performance standards, and reporting requirements • Track regulatory filings, disclosures, and approvals to ensure timely and complete submissions • Ensure systematic documentation and evidence retention to support regulatory inspections and audits • Engage proactively with MERC and relevant authorities to clarify interpretations and address compliance gaps at an early stage
		Operational & Technical	• Enforce compliance with Distribution Code, Grid Code, safety regulations, and technical standards through standard operating procedures • Integrate compliance requirements into daily operational processes, including switching, maintenance, outage restoration, and consumer service delivery • Conduct periodic technical audits, safety inspections, and field compliance reviews across divisions and circles • Implement corrective action plans for identified gaps, supported by root-cause analysis and accountability mechanisms
		Financial Compliance	• Maintain a comprehensive financial and regulatory compliance calendar with defined accountability • Institutionalize regulatory accounting & periodic reconciliation of subsidies, costs, and revenues • Ensure timely and accurate submission of ARR, MYT, true-ups, and audited financial statements • Track audit observations and loan covenant requirements through centralized action-tracking systems • Engage proactively with regulators, auditors, and lenders to address deviations at an early stage
Industry Risks	Regulatory & Policy Risks	Tariff determination	• Data-driven, transparent ARR submissions to the Maharashtra Electricity Regulatory Commission (MERC)

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
		uncertainty	• Pre-filing stakeholder consultations and scenario planning above normative parameters
		Policy volatility	• Engagement with MERC and Govt of Maharashtra on policy clarity • Regulatory horizon scanning and scenario forecasts
	Competitive and Market Risks	Pressure from alternative service providers	• Emphasis on curating innovative consumer products • Strengthen customer service (portal/helpline responsiveness to service complaints)
	Sector Transition & Technology Risks	Integration of distributed energy and renewables	• Emphasis on flexible grid architecture • Hosting capacity/feasibility studies • Advanced inverter standards & demand forecasting analytics
	Financial Risk Across the Sector	Digital transformation risk	• End-to-end cybersecurity frameworks • Phased integration approaches to avoid large systemic disruptions
Macroeconomic Risks		Persistent sector-wide financial stress	• Cost control and rational procurement • Timely tariff revision permissions to close ACS-ARR gaps • Treasury planning and efficient working capital management • Engagement with Govt of Maharashtra on predictable clearance of subsidies/dues • Cash flow modelling with stress tests tied to tariff outcomes • Communication of regulatory deferral balances and liquidity plans to stakeholders
	Economic & Financial Market Risks	Macroeconomic slowdowns	• Fixed-rate borrowing mix, hedging programmes • Demand elasticity modelling under economic slowdown scenarios
		Financial risks (including borrowing risks)	• Balanced borrowing profile; hedging strategies • Maintain minimum liquidity buffers to manage timing mismatches between revenues and power purchase obligations • Align controllable costs and capital expenditure with MERC-approved

Risk Category	Risk Sub-Category 1	Risk Sub-Category 2	Risk Mitigation
			ARR and cash flow availability • Monitor cash flows and financial variances on a regular basis to identify early stress indicators • Conduct periodic financial stress testing covering subsidy delays, AT&C loss slippages, and interest rate movements • Implement predefined financial response actions for adverse scenarios, approved at senior management level
		Borrowing risks	• Diversify funding sources to reduce dependence on any single lender or instrument • Stagger debt maturities to limit refinancing concentration in any single period • Optimize the mix of fixed and floating interest rate borrowings to manage cost volatility • Align borrowing plans with cash flow visibility, regulatory approvals, and reform milestones • Monitor covenant headroom and refinancing timelines to enable timely corrective action
	Policy & Political Risks	Subsidy and tariff issues	• Transparent reporting of subsidy flows
	Environmental & Natural Hazard Risks	National reform initiatives	• Policy dialogue with regulators and policymakers
		Weather and climate impacts	• Climate-resilient design standards (underground cabling in flood zones, stronger poles) • Emergency response protocols for monsoon/storm restoration
		Climate variability risk	• Mutual aid agreements with neighbouring utilities • Early warning and pre-deployment of repair crews

4.5. Risk Monitoring

Approved risk mitigation plans are subject to continuous monitoring to ensure effective and timely implementation. Regular updates on execution progress would be obtained, reviewed, and documented by designated stakeholders to assess adherence to agreed timelines, identify deviations, and evaluate the ongoing effectiveness of mitigation measures. This continuous oversight would support early corrective action and strengthens overall risk governance and control assurance.

4.5.1. Operational-Level Monitoring (Quarterly)

The different function heads as risk owners shall:

- Monitor Key Risk Indicators (KRIs)
- Track Mitigation Measures
- Update Risk Registers
- Escalation to Risk Management Committee

4.5.2. Organization Level Monitoring (Bi-Annual)

The Risk Management Committee shall:

- Consolidate risk inputs from all Circles and Departments
- Maintain the enterprise risk register
- Develop and update
 - ❖ Risk Dashboard
 - ❖ Mitigation tracking matrix
- Monitor cross-functional and systemic risks

4.6. Risk Review

A robust reporting and review framework would ensure that risks are systematically identified, rigorously assessed, and appropriately mitigated through well-designed controls and response mechanisms.

Periodic audits shall be conducted to evaluate compliance with approved policies and standards, and performance against such standards shall be reviewed to identify gaps, strengthen controls, and drive continuous improvement.

The organization operates within a dynamic business and regulatory environment. Accordingly, changes in internal structures, processes, technologies, stakeholder expectations, or external conditions must be proactively identified and assessed. Risk management practices shall be periodically reviewed and suitably refined to remain aligned with the evolving risk landscape.

4.6.1. Operational Function Review (Bi-Annual Review)

For operational functional review processes, the risk-owners shall not exercise final authority but shall provide structured observations and recommendations to the RMC. The different function heads as risk owners shall:

- Review enterprise risk reports prepared by the RMC

- Provide independent challenge and advisory observations on
 - ❖ Risk exposure
 - ❖ Adequacy of mitigation plans
 - ❖ Emerging regulatory or sectoral risks.
- Recommend enhancements to
 - ❖ Risk identification processes.
 - ❖ Control frameworks.
 - ❖ Risk reporting formats

4.6.2. Risk Management Committee Review (Apex Authority)

The Risk Management Committee shall:

- Conduct formal bi-annual and annual enterprise risk reviews
- Evaluate:
 - ❖ Top strategic, operational, financial, and regulatory risks
 - ❖ Residual exposure vs approved risk appetite
 - ❖ Effectiveness of enterprise-wide mitigation actions
- Approve:
 - ❖ Risk mitigation strategies
 - ❖ Resource allocation for major risk containment initiatives
 - ❖ Revisions to risk tolerance thresholds
 - ❖ Closure of risks deemed adequately mitigated
- Direct corrective action where mitigation is inadequate
- Approve updates to the Risk Management Policy

4.7. Recording & Reporting

4.7.1. Maintenance of Risk Register

All identified risks, along with their corresponding mitigation measures, would be formally documented and maintained in designated risk registers. These risk registers are subject to structured review and update on a quarterly basis to reflect changes in the internal and external operating environment, control effectiveness, and emerging risk factors.

The maintenance of up-to-date risk registers shall enable systematic tracking of risk trends and evolution over time, support timely escalation wherever required, and strengthen the organisation's ability to enhance response mechanisms, governance oversight, and overall risk management effectiveness.

5. Risk Governance

5.1. Risk Governance Structure

A well-defined risk governance structure is essential for communicating MSEDCL's approach to risk management across the organization. It ensures clarity in the allocation of roles and responsibilities

for managing risks on a day-to-day basis and embeds accountability at every level. For developing risk management framework, MSEDCL shall constitute a Risk Management Committee to be supported by Risk Cell.

5.1.1. Risk Management Committee (RMC)

It is a key group which shall adhere with the risk management framework outlined in this policy. The Risk Management Committee shall identify the key risks and report them to the functional risk owners which shall ensure that risk management activities are undertaken as per this policy.

We recognise that the merging and identified risks need to be managed and mitigated to create sustainable value for all our stakeholders and achieve business objectives.

The main objective of the Risk Management Committee shall be to provide an enterprise-wide view of key risks within the organization to the functional risk owners.

5.2. Risk reporting structure

5.2.1. Risk Management Committee of MSEDCL as per approval of the Board.

It is the final authority for approving risk treatment & mitigation plans for material risks, ensuring accountability, defined timelines, and measurable outcomes.

Composition	Reporting Line	Meeting Frequency	Responsibilities
- Chairman, Independent Director - Director (Commercial) - Director (Operations) - Director (Finance) as Invitee	Reports to the shareholders; Receives periodic briefings from the Risk Owners & Internal Audit	- Quarterly (formal) - Extra meetings when a risk escalates to higher criticality - Ad-hoc sessions for material risk events	- Oversee implementation of the risk management framework - Approve the overall risk appetite and tolerance limits - Review and validate the Risk Register, KRIs, and risk-treatment plans - Review material risks that could affect strategic objectives, financial health, or regulatory standing - Monitor the effectiveness of controls and corrective actions - Coordinate cross-functional, emerging & deteriorating risk responses - Ensure risk culture is embedded across the organization

5.2.2. Risk Owners (Business Unit /Function Heads)

It is the authority to implement agreed-upon risk-treatment actions within the unit and approve residual risk that remains within the unit's risk tolerance.

Composition	Reporting Line	Meeting Frequency	Responsibilities
-------------	----------------	-------------------	------------------

Composition	Reporting Line	Meeting Frequency	Responsibilities
• Director (Human Resource) • Director (Projects) • ED - HR • ED -Distribution • ED- Commercial • ED- Projects • ED Finance & Accounts • CGM IT	Report to their respective Directors (subjective) & Risk Management Committee (RMC)	• Review risk status in monthly unit meetings • Submit updates to RMC	• Identify risks specific to their domain (e.g., asset failure, market price volatility, regulatory changes) • Perform likelihood/impact scoring and maintain unit-level risk registers that roll-up into the enterprise register • Develop and execute treatment plans, allocate budgets, and monitor control effectiveness • Escalate any risk that crosses the pre-defined threshold to the RMC

6. Guiding Principles of Risk Management Framework

To achieve these objectives, utility should adhere to the following core principles:

- **Accountability:** The Board of Directors holds ultimate responsibility for ensuring that an effective and robust risk management process is embedded across the organization. Their oversight guarantees alignment with strategic objectives and regulatory compliance.
- **Commitment:** Every function, department, project site, and office shall collaborate seamlessly to implement this Risk Management Policy. Risk management is a shared responsibility that demands coordinated efforts across all levels of the organization.
- **Proactive & Strategic Leadership:** Risk identification including the recognition of potential lost opportunities along with risk assessment and monitoring, shall be continuous and integral to MSEDCL's operations, management practices, and decision-making processes. All identified risks must be documented and updated in a centralized risk repository for transparency and control.
- **Cultivating Strong Risk Culture:** Decisions related to risk shall be informed, consistent, and aligned with organizational objectives. Non-compliant behaviours will not be tolerated, and risk management shall be approached with professionalism and integrity at all times.
- **Transparency & Compliance:** Significant risks and associated mitigation activities shall be reported regularly. Any material failures in risk mitigation measures must be promptly escalated through the established reporting hierarchy to ensure timely corrective action and accountability.