EDC LIMITED

RISK MANAGEMENT POLICY & FRAMEWORK

(Approved in the 378th Board Meeting held on 28.10.2020)

1. **Introduction:**

EDC LIMITED (EDC) was incorporated on 12th March, 1975 as a Public Limited Company under the Companies Act, 1956 and was originally known as the Economic Development Corporation of Goa, Daman & Diu Limited. Subsequently the name of the said company was changed to EDC LIMITED on 7th September 1999. It is popularly known as EDC and is a State Financial Institution set up by the Government of Goa with prime objective of promoting Industrial Development in state of Goa.

The core business of the Company is to financially assist entrepreneur by offering a variety of loan schemes under different categories, benefitting based on, the size and nature of the project. Company provides loan to the Corporates, Government Corporations, MSMEs, unemployed youths, Government Servants under different loan schemes.

The company has also developed the Patto Plaza where many Central, State Government and Corporate houses have set up their offices.

The Company continues its drive to diversify and exploit other emerging business opportunity that lies within its business objectives.

The Company is registered with Reserve Bank of India as a Non-banking Financial Company (NBFC) without accepting public deposits vide registration No. N-13.02341 Dated 22.05.2019. The Company is deemed SFC for the purpose of exercising powers under section 29, 30 & 31 of the State Financial Corporation Act, 1951 and Financial Institution under section 2(m) of Securitisation and Reconstruction of Financial Assets and Enforcement of Security Interest Act, 2002.

2. **Background:**

Risks management is attempting to identify and manage the potential threats that could severally impact the organization and put in place various mitigation mechanism.

The Risk Management Policy of the Company is prepared considering business objectives and dynamic business environment increasing impact of various internal and external risk factors and expectations of the various stake holders. Moreover, regulatory directives and volatile economic environment and competition have brought an added focus on the risk management practices followed by the Company.

3. **Objective of this Policy:**

This risk management policy aims, to identify, mitigate and manage risk of the organization and to enable the Company to make consistently profitable and prudent business decisions and protect the reputation of the organization.

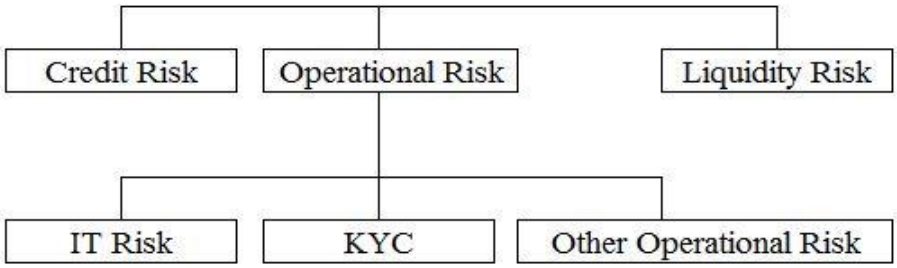
In a nutshell it seeks to ensure growth with profitability within the limits of risk absorption capacity. The objective is to facilitate the Company to acquire and maintain a pre-eminent position amongst NBFCs.

The objective of the policy is to identify the risk of the organization to mitigate and manage risk and to keep the Board of Directors and Top Management appraised of the applicable risks promptly and regularly.

4. **Risk Management Approach:**

The risk management would eventually be done at the functional/business practices, as embedded parts of their own processes, in regular day to day functioning of the company.

The Risk Management Framework of our business are detailed as under:



I. Credit Risk:

Definition

Credit Risk is defined as the risk of failure in identifying the right borrower in keeping up its commitments. It can be further described as the risk of default on a debt that may arise from a borrower failing to make required payments. The risk is that of the lender and includes lost principal and interest, disruption to cash flows, and increased collection costs.

Credit Risk Management –Objective

The objective of credit risk management is to ensure the overall health of the credit portfolio through an evaluation of the credit sanction process, credit worthiness of each customer whether new or existing, assessment of the risks involved and ensuring a measured approach to address the risks.

Credit risk in loans is managed through a strong dual combination of proper appraisal process, sufficient collateral and by timely action on non- performance of the loan account. The process of appraisal, disbursement and recovery actions is elucidated in the Manual of Standard Operating Procedures of the Corporation.

Credit risk management for all segments will include a continuous review of the existing controls and monitoring of the systems for identification and mitigation of the various risk factors.

Current Status:

The credit risk for EDC's core-business is perceived to be relatively low due to the diligent loan sanctioning process as detailed in the Standard Operating Procedure Manual and the fully secured nature of loans.

Although primarily a “fully secured” proposition, it is also recognized that risk is inherent due to adverse business/ economic conditions, the criticality of the value of collateral and the difficulty in disposal of the security at fair market value.

Way Forward:

However, with ambitious goals to achieve and with a diversified portfolio which proposes to include secured lending to the Micro, Small & Medium Segment (MSME), to Government agencies and Government employees it is imperative for EDC that the risks are identified and managed by introducing stringent credit sanctioning processes that encompass the entire gamut of the Credit Lifecycle as follows:–

- identifying of the right clientele,
- structuring of products that would suit the selected markets
- diligent credit assessment processes
- credit disbursement processes that match the best in the industry
- credit recovery strategies and processes that ensure minimal losses to the company.

Credit Risk Management

EDC will at all times have a well-structured Standard Operating Procedure encompassing the measures and precautions to be taken for Credit Risk Management that is duly supported by the Top Management and approved by the Board of Directors or by a committee appointed by them.

II. Operational Risk

Operational Risk is the risk of losses arising from failed or inadequate processes, systems, people and due to external events.

Operational Risk needs to be managed most carefully, and reviewed diligently.

Very often Operational Risks are bigger than Credit Risks and can deplete Net Worth/Capital very quickly. The allocation of appropriate levels of Capital to cover such risks has a direct influence through a higher capital costs and potentially reduce the ROA of the entire business.

Some examples of Operational Risks are as follows:

- **EMPLOYMENT BEHAVIOUR/CONDUCT:** Employee Frauds / High Attritions.
- **INFRASTRUCTURE RELATED**: Security Breaches leading to Theft / Damage to Physical Assets
- **INFORMATION SECURITY**: Data Leakages
- **INFORMATION TECHNOLOGY**: System Downtime / Access Controls / Capacity failures
- **COMPLIANCE RISKS**: Regulatory / Legal / Internal Guidelines
- **CKYC compliances.**
- **Custodial/ asset security Risk.**
- **Investment Risk.**

Operational Risk Management Framework (ORMF)

The Operational Risk Management will facilitate implementation of processes to support the proactive identification and assessment of the significant Operational Risks inherent in all products, activities, processes and systems.

The Corporation aims to achieve the following objectives:

- Meet or exceed Reserve Bank of India (RBI) requirements on Operational Risk Management in EDC.
- Assign clear accountability and responsibility for management and mitigation of Operational Risk.
- Develop a common understanding of Operational Risks, so as to assess exposure with respect to Operational Risks and take appropriate actions.
- Strengthen the internal control environment by reducing the probability and potential impact of Operational Risk losses.
- Minimizing losses and customer dissatisfaction due to failures in processes.
- Developing a loss database to collect, record and monitor Operational Risk related losses.
- Develop techniques for creating incentives to improve the management and mitigation of Operational Risks.

Information Technology Risk

This pertains to computerization data leakage, system downtime, access control, disaster recovery etc.

The Company like other similarly placed NBFCs is gradually adopting fully computerized environment for conducting its business operations. Considering the emerging challenges and business requirements the responsibility for managing the IT platform has been entrusted to its subsidiary company Goa Electronics Limited (GEL). Some of the important risk related issues in IT are listed hereunder.

a) Disaster Recovery: Data Centre (DC) & Disaster Recovery Centre (DR): The DC will be a Cloud Server to be used as a regular server and the DR will be located in the Corporation's Head Office. The Cloud Server can be remotely accessed by the employees as well as loanees for future applications if any.

b) Switch over to DR – RTO (Recovery Time Objective) / RPO (Recovery Point Objective): In order that the switchover from DC to DR and vice versa is effected quickly and efficiently issues relating to time taken for switchover and consequent data loss in transmission will be addressed periodically and defined.

c) Data Storage, Access and Backup: Database server gets updated online. Only authorized personnel will have access to the data base. Scope to tamper or alter the database are eliminated through controls. Access to data/applications are on a 'need-to-know' basis. Transaction rights are conferred only on those requiring it by virtue of the nature of their duties.

Further, access to DR site at Corporation's Head Office shall have secured access control mechanism only to authorised personnel. The Corporation has also established a Maker-Checker authorization of information systems where-in each transaction, have at least two individuals necessary for its completion. Also Audit Trail as a facility has been incorporated that ensures that the trail exist for IT assets satisfying its business requirements including regulatory and legal requirements.

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out by network administrators. Also the aforesaid Cloud Server will provide required security against loss of information.

d) Applications (Software): Only authorized and licensed software will be loaded in to the system – central and at various user points. The licensing position is to be reviewed periodically to guard against violations of IT Copyrights / Laws.

e) IT Security: A secured system of access control, both on-site and remote, including password management and secrecy will be in place and reviewed periodically. Suitable anti-virus software will be loaded in the central server and at all user points and updated regularly. A regular 'system audit' will be conducted to cover both hardware and software and the irregularities immediately addressed.

f) Cyber Security: Cyber security strives to ensure the attainment and maintenance of the security properties of the assets of the organization and its users against relevant security risks in the cyber environment. EDC shall implement security controls at all levels to protect the confidentiality, integrity and availability of information during processing, handling, transmission and storage. EDC shall endeavor to identify the various resources, including people, processes, tools and technologies, which can be utilized to prevent, reduce or manage the risk associated with a cyber incident. All existing policies related to personnel, administration, protection of confidential information, and other relevant areas would apply equally to the information resources.

g) Business Continuity Planning (BCP): BCP strives to ensure continuity, resumption and recovery of critical business processes. BCP at EDC is also designed to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster. In appropriate situations, EDC should be able to remove all its assets, documents, records of transactions and information given to the service provider from the possession of the service provider in order to continue its business operations, or delete, destroy or render the same unusable.

h) IT Services Management (Helpdesk): An efficient system to report and manage IT incidents and problems will be in place across the network of offices.

i) Responsibility: Managing IT related risks requires the commitment of the entire organization to create a safe IT environment with high level of awareness among all employees of the Corporation including the top management. The overall responsibility for managing and monitoring the IT related risks will lie with the Head of the IT Department.

Regulatory / Compliance Risk

a) **General:** The Company is an NBFC coming under the regulatory purview of the Reserve

Bank of India, and Ministry of Corporate Affairs. In addition, the Company is also required to comply with various central, state and commercial laws applicable in the conduct of the various activities of the business. Rising numbers and expectations of stakeholders, robust growth in the business of NBFCs, increasing dependency on non-equity sources of funding and some 'Corporate' frauds have increased the regulatory gaze, increased the complexity of the regulations and sometimes necessitate investments /costs.

b) **Meeting with compliance requirements**: The Company recognizes that the regulatory landscape is under periodical review and this requires the Company to be proactively prepared, as best as possible, to meet with the challenges posed by the changes. The Company will respond effectively and competitively to regulatory changes, maintain appropriate relationship with the regulators / authorities strengthen the reliance on capital and improve the quality of in-house compliance. All reports, returns and disclosures stemming from regulations will be submitted promptly and accurately to reflect the correct position. Business processes will be defined in a manner to ensure comprehensive regulatory compliance considering the multitude of regulatory agencies the Company has to deal with.

c) **Responsibility:** Competent and knowledgeable specialist officers will be recruited to ensure compliance. A specific Office Order has been issued by the Managing Director in this regards. The responsibility for ensuring compliance with regulatory requirements and directives on a day to day basis will rest with the Business Heads. The Internal Audit Department of the Company will provide the assurance through the audit of the compliance levels.

III. Liquidity Risk

Definition

Liquidity Risk is defined as the risks arising from movements in interest rates and the risk that a company of financial institution may be unable to meet short term financial demands due to the Asset Liability Mismatches. This usually occurs due to inability to convert a security to cash without a loss of capital and/or income in the process on the overall businesses of the company.

Adverse movements in interest rates could also pose a risk to the ability to raise funds for managing liquidity gaps – giving rise to Liquidity Risks.

Responsibility

At the Management Level, our Corporation has a Resources Department which manages the Fund Management and Treasury Operations so as to ensure sufficient liquidity for the Corporation. We have also formed The Asset Liability Management Committee (ALCO) of EDC – at the Management Level, The Audit committee of the Board as well as the Risk Management Committee of the board, at the Board Level, to closely monitor any Asset Liability mismatches, Liquidity positions and the macro-environment to consider all indicators of risks, to plan and advise suitable action.

5. Risk Governance in EDC

The Risk Governance structure for EDC will be both at the Board level and at the Management level.

Key Principles of Risk Governance

EDC's risk governance framework is based on the following key principles:

While the Board of Directors will be responsible for overall governance and oversight of core risk management activities, execution strategy will be delegated to the Risk Management Committee of the Board (RMCB) and further sub-delegated to the Management Level Risk Committees namely, the Asset Liability Management Committee (ALCO), Preliminary Clearance Committee, 2D Committee, GM Committee, etc.

All major risk classes are managed through focused and specific risk management processes; these risks include credit risk, market risk, operational risk and liquidity risk. As EDC gains sophistication in risk management, it shall put in place advanced risk management models commensurate with the size, scale and complexity of its business.

Policies, processes and systems shall be put in place to enable the risk management capability

The Risk related department/ function shall have appropriate representation on

management committees of EDC to ensure that relevant risk view is taken in to consideration in business decisions and monitoring and processes shall be established to monitor the performance against approved risk appetite.

Risk Management Committee of the Board (RMCB):

The RMC is constituted as under:

1. Any Independent Director, EDC ….. Chairperson
2. Jt. Managing Director & CGM … Members
3. GM– Loans/Recovery/Accts./Resources/Legal/Computer Cell …. Members
4. Chief Information Security Officer (CISO) …Member
5. Ombudsman Official…Member
6. Compliance Officers – DGM (Accts) and Manager (Accts.) …Member
7. Principal Officer and Designated Director…Member
8. Fraud Risk Management Official…Member
9. Company Secretary …Member

Company Secretary shall be the Member Secretary

Frequency of Meeting

The RMCB shall meet at least 2 times in a financial year

Roles and Responsibilities of the RMCB

The key responsibilities of the Risk Management Committee of the Board (RMCB) include:

1. Approve / recommend to the Board for its approval / review of the policies, strategies and associated frameworks for the management of risk.
2. Approve the risk appetite and any revisions to it.
3. Sub-delegate its powers and discretions to executives of EDC, with or without power to delegate further.
4. Ensure appropriate risk organization structure with authority and responsibility clearly defined, adequate staffing, and the independence of Risk Management functions.
5. Provide appropriate and prompt reporting to the Board of Directors in order to fulfill the oversight responsibilities of the Board of Directors.
6. Review reports from management concerning EDC's risk management framework (i.e. principles, policies, strategies, process and controls) and also discretions conferred on

executive management, in order to oversee the effectiveness of them.

7. Review reports from management concerning changes in the factors relevant to EDC's projected strategy, business performance or capital adequacy.
8. Review reports from management concerning implications of new and emerging risks, legislative or regulatory initiatives and changes, organizational change and major initiatives, in order to monitor them.
9. Ensure adherence to the external, internal policy guidelines and also regulatory guidelines.
10. Oversee statutory / regulatory reporting requirements related to risk management.
11. Monitor and review capital adequacy computation with an understanding of methodology, systems and data.
12. Monitor and review of non-compliance, limit breaches, audit / regulatory findings, and policy exceptions with respect to risk management.
13. The RMCB will be responsible for reviewing and confirming order/decisions of identification of willful defaulters given by the Central Credit Committee.

6. Risk Reporting

Risk Management will not be completed without a structured process for reporting of risk related information, to all its stake holders.

Risk Reporting therefore has two significant categories – Reporting to External Stakeholders and Reporting to Internal Stakeholders.

Risk Reporting to External Stake holders:

External Stakeholders are always regulatory and legislative bodies. As a Financial Institution, classified as a "Systemically Important" (SI), there are many reports to be submitted on risk related information – mainly from the Credit Risk side to regulators like RBI but on the whole, these reporting cover an all round perspective of risks of the Company.

Risk Reporting to Internal Stakeholders

The Company Secretary will advise all internal stakeholders on the relevant and extant reporting to be followed, from time to time.

Internal stakeholders are primarily

1. Board of Directors
2. Committees of the Board
3. Top Management Team
4. Functional Management Teams

Thus, Risk Reports to Internal stakeholders can be classified as

- Strategic Reports on Risks – i.e. Reports that help formulate or review strategies
- Tactical Reports on Risks – i.e. Reports that help review the need for course-corrections
- Functional Reports on Risks – i.e. Reports that help measure the risk- metrics in a structured and consistent manner across all functional units of the company, and those that become the basic source of any MIS reports on Risks of the Company.

****