

NIHON

NIHON IMPEX PRIVATE LIMITED

RISK RATING POLICY

Risk rating involves the categorization of individual loans, based on credit analysis and local market conditions, into a series of graduated categories of increasing risk. Risk ratings are most commonly applied to all loans other than personal and residential mortgage/bridge loans.

Risk ratings should be conducted:

- at the time of application for all new or increased loan facilities
- as part of the annual review process
- in situations where new information is considered that may materially affect the credit risk of the loan

A primary function of a risk rating model is to assist in the underwriting of new loans. As well, risk rating assists management in predicting changes to portfolio quality and the subsequent financial impact of such changes. Risk rating can also lead to earlier responses to potential portfolio problems, providing management with a wider choice of corrective options and decreased exposure to unexpected credit losses. Finally, risk ratings are useful for pricing loans and regulating the commercial portfolio exposure to maximum levels of risk.

In many situations, however, a system comprised of six risk levels of increasing credit risk is appropriate. Under this system, the lowest risk rating (1) is assigned to undoubted borrowers with virtually no risk. The highest risk rating (6) is assigned to borrowers where there is little or no likelihood of repayment. Loans should only be granted for risk ratings of 1, 2 (low risk) or 3 (normal risk). Ratings of 4, 5 and 6 are reserved for existing loans where the risk rating has deteriorated from the time of the original approval. Risk rating 4 is a “cautionary” rating assigned to higher risk loans.

RISK RATING POLICY

1. PREAMBLE

A risk rating policy helps equip the digital lender to support a diverse crowd of borrowers across industries and income levels. The classification on varied risk ratings ranging from very high to very low helps the financial institution make decisions that are useful and credible once customer KYC is done.

2. DEFINITION AND OBJECTIVES

Risk: Risk is an event which can prevent, hinder, or fail or otherwise obstruct, the enterprise in achieving its objectives. A business risk is the threat that an event or action will adversely affect an enterprise’s ability to maximize stakeholder value and to achieve its business objectives. Risk can cause financial disadvantage, for example, additional costs or loss of funds or assets. It can result in damage, loss of value and /or loss of an opportunity to enhance the enterprise operations or activities. Risk is the

product of probability of occurrence of an event and the financial impact of such occurrence to an enterprise.

The objective of this Policy is to manage the risks involved in all activities of the Company, to maximize opportunities and minimize adversity. This Policy is intended to assist in decision making processes that will minimize potential losses, improve the management of uncertainty and the approach to new opportunities, thereby helping the Company to achieve its objectives. The objectives of the Policy can be summarized as follows:

- a) To safeguard the Company's and its subsidiaries' / joint ventures' property, interests, and interest of all stakeholders;
- b) To protect and enhance the corporate governance;
- c) To implement a process to identify potential / emerging risks;
- d) To manage risks with an institutionalized framework and consistently achieving desired outcomes;
- e) To implement appropriate risk management initiatives, controls, incident monitoring, reviews and continuous improvement initiatives;
- f) To minimize undesirable outcomes arising out of potential risks; and
- g) To align and integrate views of risk across the enterprise.

3. RISK MANAGEMENT COMMITTEE

The Risk Management Committee shall have minimum three (3) members with majority of them being members of the Board of Directors, including at least two thirds of members of the Risk Management Committee shall comprise independent directors. The Chairperson of the Risk Management Committee shall be a member of the Board of Directors and senior executives of the Company may be members of the Risk Management Committee.

The RMC shall meet on a regular basis not less than a meeting shall be held half-yearly. The quorum for a meeting of the Risk Management Committee shall be either two (2) members or one third of the members of the Risk Management Committee, whichever is higher, including at least one member of the Board of Directors in attendance.

4. RISK MANAGEMENT PROCESS

Conscious that no entrepreneurial activity can be undertaken without assumption of risks and associated reward opportunities, the Company operates on a risk management process/framework aimed at minimization of identifiable risks after evaluation so as to enable management to take informed decisions.

Broad outline of the framework is as follows:

- a) **Risk Identification:** Management identifies potential events that may positively or negatively affect the Company's ability to implement its strategy and achieve its objectives and performance goals. The categories of risk are identified by the Management and updated to the RMC on a periodic basis.
- b) **Root Cause Analysis:** Undertaken on a consultative basis, root cause analysis enables tracing the reasons / drivers for existence of a risk element and helps developing appropriate mitigation action.
- c) **Risk Scoring:** Management considers qualitative and quantitative methods to evaluate the likelihood and impact of identified risk elements. Likelihood of occurrence of a risk element within a finite time is scored based on polled opinion or from analysis of event logs drawn from the past. Impact is measured based on a risk element's potential impact on revenue, profit, balance sheet, reputation, business and system availability etc. should the risk element materialize. The composite score of impact and likelihood are tabulated in an orderly fashion. The underlying model to arrive at the composite score for various categories of the risk shall be deployed internally in the Company in a graduated manner. The resultant "action required" is derived based on the combined effect of impact & likelihood and is quantified as per the subsequent paragraphs.
- d) **Risk Categorization:** The identified risks are further grouped in to (a) preventable; (b) strategic; and (c) external categories to homogenize risks.
- Preventable risks are largely internal to the Company and are operational in nature. The endeavour is to reduce /eliminate the events in this category as they are controllable. Standard operating procedures and audit plans are relied upon to monitor and control such internal operational risks that are preventable.
 - Strategy risks are voluntarily assumed risks by the senior management in order to generate superior returns / market share from its strategy. Approaches to strategy risk is 'accept'/'share', backed by a risk-management system designed to reduce the probability that the assumed risks actually materialize and to improve the Company's ability to manage or contain the risk events should they occur.
 - External risks arise from events beyond organization's influence or control. They generally arise from natural and political disasters and major macroeconomic shifts. Management regularly endeavours to focus on their identification and impact mitigation through 'avoid'/'reduce' approach that includes measures like business continuity plan / disaster recovery management plan / specific loss insurance / policy advocacy etc.

- e) Risk Prioritization: Based on the composite scores, risks are prioritized for mitigation actions and reporting.
- f) Risk Mitigation Plan: Management develops appropriate responsive action on review of various alternatives, costs and benefits, with a view to managing identified risks and limiting the impact to tolerance level. Risk mitigation plan drives policy development as regards risk ownership, control environment timelines, standard operating procedure, etc.

Risk mitigation plan is the core of effective risk management.

The mitigation plan covers:

- Required action(s);
- Required resources;
- Responsibilities;
- Timing;
- Performance measures; and
- Reporting and monitoring requirements

The mitigation plan may also covers (i) preventive controls - responses to stop undesirable transactions, events, errors or incidents occurring; (ii) detective controls - responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken; (iii) corrective controls - responses to reduce the consequences or damage arising from crystallization of a significant incident.

Therefore, it is drawn with adequate precision and specificity to manage identified risks in terms of documented approach (accept, avoid, reduce, share) towards the risks with specific responsibility assigned for management of the risk events.

- g) Risk Monitoring: It is designed to assess on an ongoing basis, the functioning of risk management components and the quality of performance over time. Staff members are encouraged to carry out assessments throughout the year.
“Fraud & Operations Risk” team works on a robust and dynamic real-time transaction monitoring mechanism via an automated rule engine already in place. This engine functions basis predefined set of rules. Our Operations Risk team comprises Risk Experts and Data Scientists who evaluate and monitor merchant transaction and market trends to raise alerts which are actioned as per the alert monitoring protocols.
- h) Options for dealing with risk: There are various options for dealing with risk.
 - Tolerate – If we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk; i.e., do

nothing further to reduce the risk. Tolerated risks are simply listed in the corporate risk register.

- Transfer – Here risks might be transferred to other organizations, for example by use of insurance or transferring out an area of work.
- Terminate – This applies to risks we cannot mitigate other than by not doing work in that specific area. So, if a particular project is of very high risk and these risks cannot be mitigated we might decide to cancel the project.

- i) Risk Reporting: Periodically, key risks are reported to the RMC with causes and mitigation actions undertaken/ proposed to be undertaken.

The internal auditor carries out reviews of the various systems of the Company using a risk based audit methodology. The internal auditor is charged with the responsibility for completing the agreed program of independent reviews of the major risk areas and is responsible to the audit committee which reviews the report of the internal auditors on a quarterly basis.

The statutory auditors carries out reviews of the Company's internal control systems to obtain reasonable assurance to state whether an adequate internal financial controls system was maintained and whether such internal financial controls system operated effectively in the company in all material respects with respect to financial reporting.

On regular periodic basis, the Board will, on the advice of the audit committee, receive the certification provided by the CEO and the CFO, on the effectiveness, in all material respects, of the risk management and internal control system in relation to material business risks.

The Board shall include a statement indicating development and implementation of a risk management policy for the Company including identification of elements of risk, if any, which in the opinion of the Board may threaten the existence of the Company.

- j) Risk Management Measures adopted in general by the Company: The Company has adopted various measures to mitigate the risk arising out of various areas described above, including but not limited to the following:

- A well-defined organization structure;
- Defined flow of information to avoid any conflict or communication gap;
- Hierarchical support personnel to avoid work interruption in absence/ non-availability of functional heads;

- Discussion and implementation on financial planning with detailed business plans;
- Detailed discussion and analysis of periodic budgets;
- Employees training and development programs;
- Internal control systems to detect, resolve and avoid any frauds;
- Systems for assessment of creditworthiness of existing and potential contractors/subcontractors/ dealers/vendors/ end-users;
- Redressal of grievances by negotiations, conciliation and arbitration; and
- Defined recruitment policy