Maheshwari Equity Services (P) Limited
Kolkata – 700 001

Risk Management & Due Diligence

Policy

of

Maheshwari Equity Services (P) Limited
(Stock Broking Services)

Policy Reveiwed on 03-Apr-2023

Maheshwari Equity Services (P) Limited
Kolkata – 700 001

Overview

Every Organization uses information, most are dependent on it. Various risks may affect the security - confidentiality, integrity and availability - of this information. Information security is founded on risk management because total security is unaffordable and probably unachievable. Information security is not an 'IT problem', it is a business issue. Risks are managed by reducing their likelihood and or mitigating their business consequences. The purpose of this Guideline is to assist Risk Management & due diligence.

The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures are required under the various United Nations Security Council Regulations which can be accessed at:

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml
http://www.un.org/sc/committees/1988/list.shtml

Purpose:

A risk categorization is required to understand the threats which could be materialized and the impact they would have on the organization.

Scope:

This policy covers all kinds of business risk related to Information of client financial strength, security and applies to all information system infrastructure and their users i.e. all members of the organizations.

Definitions:

Threats: A hazard is anything that can go wrong or cause harm e.g. unauthorized trade or over limit trade etc. The impacts of hazard materializing vary but they normally result in direct and indirect financial loss, in some cases reputation/brand damage and even, following severe incidents for which the organization is unprepared, failure of the organization to survive.

Risk: A risk consists of two components:

- the likelihood or probability that a particular threat will materialize
- the impact or consequences that might result, hence a risk is a measure of how likely a threat is to impact the organization given the level of control in place to avoid or manage the threat.

Maheshwari Equity Services (P) Limited
Kolkata – 700 001

Control: A control is a means by which the likelihood of a threat materializing or the impact of the threat should it materialize is reduced. Controls come in many forms but can include fire suppression systems, security access controls, an effective off-site data backup regime, manual workarounds for key processes, use of multiple offices to spread risk etc. Controls need to be cost-effective and appropriate to the risk faced.

Information assets: All hardware, software, systems, services, personnel, information (printed and/or electronic) and any other related technology assets that are important to the business.

Sensitive assets:

Information assets that require protection against unavailability, unauthorized access, or disclosure. Sensitive information assets may be confidential and/or critical.

Potential exposures to RISK may be classified as:

- Facility Related: Bomb Threat, , Civil Disturbance, Electrical Failure, Fire, , Water Leaks, Work Stoppage / Strike
- Technology Related: Human Error, Loss of Telecommunications, Data Center Outage, Lost / Corrupted Data, Loss of Local Network Services, Power Failure, Prolonged Technology Outage, UPS / Generator Loss of service.
- Nature Related: Earthquake, Flood / Flash Flood, Hurricanes / Tropical Storms, Severe Thunderstorms, Tornado, Winter Storms

Responsibility:

This policy provides guidelines for procedures and responsibilities for management, system administrators and users. All staff must understand and accept the need for Risk assessment and it should be seen as a common responsibility. All Staff members can raise their concerns or report observations.

As per the SEBI notification no. LAD-NRO/GN/2010-11/21/29390 published on December 10, 2010 guidelines, persons associated with a registered stock-broker/trading member/clearing member who are involved in, or deal with, any of the below mentioned functions are required to have a valid NISM Series VII Certification Securities Operations and Risk Management Certification.)

(a) Assets or funds of investors or clients,
(b) Redressal of investor grievances,
(c) Internal control or risk management, and
(d) Activities having a bearing on operational risk,

Maheshwari Equity Services (P) Limited
Kolkata – 700 001

However, in view of the operational difficulties it has been decided that requirement of passing of NISM Series VII - Securities Operations and Risk Management Certification exam would be optional for associated persons of a registered stock-broker/trading member/clearing member handling the basic clerical/elementary functions as explained in the Exchange circular no. NSE/INSP/27495 dated September 2, 2014

Indicative activities falling under basic elementary level/clerical level

Internal control or risk management

1. Inwarding of collateral's/cheques
2. Person performing maker entries
3. Maker entry in the database
4. Photocopying, printouts, scanning of documents
5. Preparing of MIS
6. Sending of letters/reports to clients, Exchanges, SEBI
7. Attending calls, etc.

Redressal of investor grievances

1. Inwarding of complaints,
2. Seeking documents from clients
3. Person performing maker entries
4. Maker entry in the database
5. Photocopying, printouts, scanning of documents
6. Preparing of MIS
7. Sending of letters/reports to clients, Exchanges, SEBI Updation, data entry, uploading on SCORES.
8. Attending calls, etc.

Activities having a bearing on operational risk and dealing with assets or funds of investors or clients

1. Person performing maker entries
2. Maker entry in the database
3. Preparing MIS
4. Generating reports, Files
5. Photocopying, printouts, scanning of documents
6. Dispatching documents to clients
7. Sending of letters/reports to clients, Exchanges, SEBI
8. Attending calls, etc.

Policy Reveiwed on 03-Apr-2023

Maheshwari Equity Services (P) Limited
Kolkata – 700 001

Procedures:

Assessing Risk:

- Identifying – Risk, hazards and threats
- Prioritize Risks- top the risks who will more affect the critical assets and activities
- List and Define Risk- in a sequential manner with a brief explanation to each
- Probability - of Occurrence of a threat/ hazard
- Vulnerability- to Risk of critical activities
- Potential -Impact on Organization and its resources and business
- Set- Risk Appetite
- Preventative -Measures in Place to control the risk
- Carry out a cost benefit analysis
- Insurance Coverage – transfer of risk
- Past Experiences
- Design - Business Continuity Strategy to maximize operational resilience.

As per our internal policy, we have bifurcated clients under 3 categories of risk.

High Risk: The clients mapped under this category are not given the delivery of their shares till their debits are cleared and a fresh exposure is allowed only till T+5 days after which the limits are blocked till a confirmation of clearance of the debits is received from the clients.

Medium Risk: The clients falling under this risk group are given the share delivery wherein the maximum ledger debit is up to Rs. 50000.00. Exposures are given on the basis of margins.

Low Risk: These clients are well known to the company on the basis of their track record. Hence their debits up to a maximum of Rs. 1000000.00 are allowed. Simultaneously exposures granted to them are a bit flexible in nature (2 times more the normal exposure norms) on the basis of available margins. Clients who do not want the shares to be delivered to their demat account and utilize the same for limit / exposure by keeping the shares in our holdback account are also mapped under this category.

Policy Reveiwed on 03-Apr-2023

Maheshwari Equity Services (P) Limited
Kolkata – 700 001

Analyzing the results:

Review and Interview Notes

Implement Risk Management Control Program – where proposed solutions are easily implemented

Follow-up meetings of management and departments related for other solutions the decision on what to do and when to do it

Look for an economic balance between the impact of each risk and the cost of security solutions intended to manage it.

Report the Results - Each departmental business impact analysis/risk assessment team is expected to complete a report that can be easily shared with those parties involved in the process

Final Report & Presentation:

Presenting the Results-The departmental business impact analysis/risk assessment team will meet as needed to review what work has been accomplished and to discuss specific strategies. This review will be determined by actions taken or a possible major change in technology. The team should record what has been done to address specific risks and maintain for a "year-ending" report to management.

Next Steps - This report and presentation can also be used to address new issues and to consider if any risks might need to be discussed on a organization -wide basis.

Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Conclusion:
Risk assessment is important tool to protect human resources and business of the organization; it should be reviewed on an ongoing basis and kept up to date and effective.