

CHOICE EQUITY BROKING PVT. LTD**IS Risk Management Methodology****Version Control**

Action	Date	Revision Details	Prepared / Amended By	Changes
Created On	24-Aug-2024	1.0	GRC Consultant	Initial Draft
Reviewed On	24-Aug-2024	1.0	Shripad Mayekar Information Security Manager	Initial review
Approved on	1-Sep-2024	1.0	Ashutosh Bhardawaj-CISO	Approved
Reviewed On	28-Jan-2025	1.1	Shripad Mayekar Information Security Manager	updated as per ISO stage 1 audit requirements
Approved on	20-Feb-2025	1.1	Ashutosh Bhardawaj-CISO	Approved

Table of Contents

1. Introduction	2
2. Risk Management Methodology	3
2.1 Communication and consultation	3
2.2 Risk Criteria/Triggers	4
2.3 Risk Assessment	5
2.3.1 Risk Identification	5
2.3.2 Risk Analysis	6
2.3.3 Risk Evaluation	8
2.4 Risk Treatment	9
2.5 Risk Monitoring and Review	10
3. Maintenance of Risk Management Methodology	12
4. References	13

1. Introduction

- It is essential for every organization to have a clearly defined, comprehensive and repeatable risk management program. This document defines the methodology for identification, classification, treatment and monitoring of information security risks at Choice.
- This risk management methodology should be adopted and implemented while assessing, treating and managing risks associated with the information assets and information processing facilities of Choice.
- This methodology sets out a pro-active, semi-quantitative approach for systematically addressing the existing risks throughout the lifecycle of information and information processing facilities of Choice.

2. Risk Management Methodology

Risk Management methodology is a continual process that involves the following key steps:

1. Communication and consultation
2. Establishing the context
3. Risk Assessment
 - Risk Identification
 - Risk Analysis
 - Risk Evaluation
4. Risk Treatment
5. Risk Monitoring and review

This methodology should be followed to ensure that the Choice approach to risk management is both comprehensive and consistent. All steps of this methodology should be formally conducted across the entire organization on an annual basis or when significant changes are proposed or occur. Further, risk management would not solely be an annual process and should be performed at all times and in relation to all activities affecting information security. Therefore, everyone shall have a responsibility to continually apply this methodology when making business decisions and when conducting day-to-day management.

Based on below risk matrix, risk would be assessed and treated:

TYPE OF RISK	RANGE OF RISK VALUES	ACCEPTABLE RISK VALUE
1. Residual Risk 2. Inherent Risk	1. High (H) 2. Medium(M) 3. Low (L)	1. Low (L)

2.1 Communication and consultation

Choice should communicate and consult with the internal and external stakeholders throughout the risk management lifecycle to ensure that the organization has a comprehensive picture of the existing risks and mitigation steps.

External communication and consultation is targeted at communicating following with external stakeholders (including Government and Industry):

1. The organization's risk management approach;
2. The effectiveness of risk management approach; and
3. Requesting feedback where appropriate.

Internal communication and consultation is aimed at communicating following with internal stakeholders:

1. The risk management process;
2. Seeking feedback in relation to the process; and
3. Key risks and their responsibilities relating to management of the process.

2.2 Risk Criteria/Triggers

Risk assessments will be initiated whenever specific criteria or triggers occur that indicate a potential threat to the organization's operations, assets, or compliance obligations.

Changes in Business Strategy or Objectives:

- Any significant changes to the organization's strategic direction, new business initiatives, mergers, acquisitions, or expansion into new markets.

Organizational Change (Leadership or Structural):

- Change in key leadership (e.g., CEO, CFO, CIO), significant structural reorganizations, or departmental shifts.

Introduction of New Technology or Systems:

- The organization is introducing new technologies (e.g., software, hardware, cloud services) or systems (e.g., new trading platforms, ERP systems, or customer relationship management systems).

Regulatory or Legal Changes:

- New or updated laws, regulations, or compliance standards (e.g., IT Act, SEBI Act, financial regulations, cybersecurity frameworks)..

Audit Findings or Internal Controls Weaknesses:

- Identified major weaknesses, deficiencies, or major non-compliance issues during internal audits, external audits, or self-assessments.

Incident, Breach, or Operational Failure:

- A security breach, data leak, failure of critical systems, or any significant operational disruption (e.g., cyberattack, supply chain failure, system outage).

Supply Chain Disruptions or Dependencies:

- Disruptions in the supply chain (e.g., vendor failure, shipping delays, raw material shortages), or changes in critical third-party suppliers or partners.

High-Impact Environmental or External Factors:

- External environmental factors, such as changes in the market, political instability, natural disasters, or economic downturns.
- Action: Trigger a risk assessment to understand the external risks that could potentially impact your business operations, financial stability, or reputation.

New or Emerging Threats (Cybersecurity or Physical Threats):

- Discovery of new or emerging threats in cybersecurity, fraud, or physical security (e.g., malware attacks, ransomware trends, physical security vulnerabilities, data theft).

Third-Party Risk:

- Issues related to third-party vendors, such as data breaches, non-compliance, or performance failures.

2.3 Risk Assessment

Risk assessment is a careful examination of risks, its cause, probability of risk occurrence and impact which may affect, cause loss or damage to information and information systems managed by Choice. Risk Assessment shall be performed in accordance with the defined Scope in ISMS.

Risk assessment involves:

1. Risk Identification
2. Risk Analysis
3. Risk Evaluation

2.3.1 Risk Identification

Risk identification is a key step in the risk assessment process to ensure a complete list of risks is identified.

1. Choice should identify risk sources, areas of impact, causes and possible consequences to form a comprehensive list of risks based on events that might create, enhance, prevent, degrade, accelerate or delay the achievement of an organization's objectives. Comprehensive identification of risks is critical, because risks that are not identified at this stage would not be

included in further analysis. Risks can be identified using various tools and techniques including, but not limited to the following,

- Audit reports
- Checklists
- Strategic and business plans
- Structured interviews
- Surveys and questionnaires
- Self-observations and experiences
- Project plans
- Architectures

2. Risk identification step should capture following:

Risk Identification								
SR No	Risk	Cause	Risk Context	Location	Department	Asset	Risk Category	Risk Owner
#N o	Enter the Identified Risk	Describe the potential causes of event occurring	Identify the type of the Risk Context	Name of the Location	Name of the Department	Identify the Assets relevant to the risk identified	Identify the relevant risk category	CHOICE INDUSTRIES LTD (Risk Owner for each identified risk)

- Enter the identified risk – Document the risks after considering the external and internal factors along with the help of various tools and techniques ;
- Identification of potential causes – Determine the causes that could lead to risks.
- Identification of risk content – Internal / External factor;
- Affected locations – e.g Choice Head Office, Hyderabad, etc.
- Affected assets – Affected assets should be categorized as Physical / Software / Information / Document / Service / People;
- Categorizing the risk – Risk should be categorized based on their nature : Business Continuity / Infrastructure Assets & Systems / Environmental / Financial / Reputation / Operational / Compliance
- Owner of the risk – Based on the locations and responsibilities, risk owner(s)

2.3.2 Risk Analysis

Risk analysis involves identifying and assessing the effectiveness of the existing controls (automatic/manual) to manage the risk, by either reducing the consequence or likelihood of the risk. Risk analysis step should capture the following details:

Risk Analysis			
Existing Control / Current Measure	Control Assessment	Likelihood	Impact

List of existing control	Effectiveness of the existing control	Assess the probability of risk event occurring	Assess the possible impact of risk event occurring
--------------------------	---------------------------------------	--	--

- List of existing controls: The existing controls should be captured against all in-scope business processes that are currently being protected against the identified risks.
- Effectiveness of the existing control: On application of existing controls, the effectiveness of the existing controls should be evaluated based on its performance – Effective / Adequate / Marginal / Deficient. Existing controls can be evaluated through several different processes including:
 - a. Control self-assessment;
 - b. Internal Audit reviewing the effectiveness of controls; and
 - c. External Audit reviewing the effectiveness of controls.
- The definition for the effectiveness value is as follows:

Control Assessment			
Any action or activity that the firm has in place that either reduces the likelihood of a risk event occurring or minimizes the potential for impact arising from that event.			
RATING	Design	Performance	Description
Effective	Designed to reduce risk entirely	Control is always applied as intended	The design and the performance of the controls are considered sufficient
Adequate	Designed to reduce most aspects of risk	Control is generally operational but on occasions is not applied as intended	Minor weaknesses exist in the design or in the performance of the control
Marginal	Designed to reduce some area of risk	Control is sometimes applied correctly	Deficiencies exist in risk mitigation / controls
Deficient	Very limited or badly designed, even where used correctly provides little or no protection	Control is not applied or applied incorrectly	Limited controls and/or management activities are in place, high level of risk remains.

- Likelihood of the risk: Based on the existing control, assess the probability of risk event occurring as Frequent / Possible / Rare. The definition of the likelihood ratings is as follows:
- The potential for risk to occur is only indicative and individual risk need to be rated for likelihood in its specific context with appropriate judgement.

Likelihood	
The probability of risk occurring:	
RATING	POTENTIAL FOR RISK TO OCCUR
Frequent	Likely to occur several times a year
Possible	Possibly occurs once a year or 2 years

Rare	Possibly occurs once 5- 10 years
------	----------------------------------

- Impact of the risk: Impact of the risk should be based on the effectiveness of the existing controls for the identified risks. The impact should be captured as major / moderate / Incidental. The definition of the impact ratings is as follows:

Impact level	Confidentiality	Integrity	Availability
Major	Unauthorized access to highly sensitive data such as financial data, trading strategies, customer portfolios. Major impact to firm (e.g., financial loss > INR 1 crore reputational damage, regulatory penalties, and legal action).	Major discrepancies in financial transactions, trading algorithms, or critical customer accounts. Could lead to >INR 1 crore loss, regulatory fines, and loss of client trust.	Full system downtime affecting trading platforms, order processing, or access to accounts. Results in >INR 1 crore losses, regulatory non-compliance, and loss of market position.
Moderate	Sensitive data exposed. Breach results in medium to high-level reputational damage, compliance issues, and potential for INR 50 Lakh to INR 1 crore financial loss.	Inaccurate or altered data in customer accounts or trading logs, potential fines between INR 50 Lakh and INR 1 crore . Some operational disruption.	Partial downtime or degraded performance of trading systems leading to delays or order issues, with a moderate financial impact but manageable losses(~INR 50 Lakh - INR 1 crore).

Incidental	Access to non-sensitive data leading to reputational damage or compliance issues but no regulatory consequences. Financial loss under INR 50 Lakh.	Minor discrepancies in customer accounts or trade logs requiring manual correction and causing minor operational disruption. Financial loss under INR 50 Lakh.	Partial downtime or degraded performance affecting non-critical platforms, causing delays or minor disruptions without significant revenue loss. Financial loss under INR 50 Lakh
-------------------	--	--	---

Examples of categories of data are listed below:

Data Category	Highly Sensitive Data	Sensitive Data	Non-Sensitive Data
Customer Data	Full Names, PAN, Adhar no, Tax Identification Numbers (TINs)	- Client Portfolios (detailed stock holdings, bonds, etc.)	- Public Contact Information(phone number, address)
	- Bank Account Details (linked to accounts)	- Transaction History (specific buy/sell orders, amounts)	- General Demographic Data (age range, location, etc.)
	- Personal Identification Details (DOB, mother's maiden name)	- Trading Preferences (risk tolerance, asset allocation)	- Public Events/Notices (news, ads, marketing materials)
	- Login Credentials (username, password, 2FA tokens)	- Account Balances	- Public Website Information (company contact, services)
Financial Data	- Client's Detailed Financial Statements (assets, liabilities)	- Detailed Account Information (e.g., account balances, margin status)	- Stock Price History(open, close, volume)
	- Trade Secrets or Proprietary Algorithms	- Limited Transaction Data (e.g., aggregate monthly transactions)	- Public Financial Reports (e.g., quarterly results)

Operational Data	- Internal Trading Algorithms (secret formulas, strategies)	- Internal Market Data (non-public pricing feeds)	- System Logs (non-sensitive operational logs)
-------------------------	---	---	--

- The consequence and likelihood ratings, as identified after consideration of existing controls, are combined to determine the overall inherent risk level based on below matrix:

Risk Evaluation Criteria			
LIKELIHOOD		IMPACT/CONSEQUENCE	
	Frequent	6	9
Possible	2	4	6
Rare	1	2	3
	Incidental	Moderate	Major

2.3.3 Risk Evaluation

Risk evaluation step should evaluate the risk with existing controls and method to treat the same. Risk evaluation step should capture the following:

Risk Evaluation		
Inherent Risk	Inherent Risk Level	Risk Treatment Option
Inherent risk post prevention controls	Inherent Risk Level	Describe the treatment to be applied to risk

- Inherent risk post prevention controls: Based on evaluation of the existing controls, likelihood and risk impact ratings, the inherent risks that exists even after the application of the current controls has to be documented.
- Inherent Risk Level: The value of inherent risk is automatically calculated based on the likelihood and impact ratings.

$$\text{Risk Level (potential / residual)} = \text{Likelihood} * \text{Consequence}$$

Below table depicts the Risk Level based on likelihood and consequence of the risk:

Level of Risk		
The ranking assigned after considering the likelihood and consequence of a risk		
Risk Level	Activity	Range
High	Needs Action	7-9
Medium	Needs Attention / Improvement	4-6
Low	Monitoring Needed - Annually	1-3

*Range values are obtained from the risk evaluation criteria table.

- Risk treatment option: Depending upon the risk level ratings and existing controls, the risk can be treated in the following ways: Avoid / Reduce / Share / Accept. If the risk level is low, then we would accept the risk. The definition of the treatment values are as follows:

Risk Treatment Option	
Depending on the type and nature of the risk, the following options are available:	
Option	Treatment
Avoid	A strategy to control risk by eliminating the possibility of loss by exiting any activity that would expose the company/project/ business unit to a loss (e.g.. don't take up a risky activity)
Reduce	A strategy to defer action and maintain the current impact and probability of a risk until it rises above an acceptable level
Share / Transfer	A strategy to reduce the probability and/or negative impact of a risk to an acceptable level (e.g. Training)
Accept	A strategy to remove the risk from the risk portfolio by eliminating risk drivers and activities (e.g. Insurance)

2.4 Risk Treatment

Risk treatment is the process to make decisions on risks which can be reduced, accepted, avoided and transferred. The risk treatment plan should be implemented, in order to achieve the identified control objectives. Risk treatment phase should capture the following details:

Risk Treatment/ Action Plan		
Risk Treatment Action/Plan		Timelines
Steps to treat the risk	ISO 27001 Reference	Specify the period of resolution

- Steps to treat the risk: Based on the risk treatment option selected during the risk evaluation stage, the risk with the risk value as high and medium shall be addressed with appropriate risk treatment measures. For the risks having lower risk values, minimum safeguards should be put in place for ensuring security of the information.
- ISO 27001:2022 Reference: The risk treatment controls shall be mapped to the ISO 27001:2022 standard controls.
- Specify the timeliness: The period required for resolving and mitigating the risks should be specified.

2.5 Risk Monitoring and Review

The risk value remaining after treatment (residual risk), should be accepted based on the risk acceptance criteria. Risk monitoring and review should capture the following details:

Risk Monitoring & Review

Residual Risk	Residual Risk Likelihood	Residual Risk Impact	Residual Risk Level	Risk Acceptance	Plan/Justification for Residual Risk	Risk Treatment Status	Remarks
Residual Risk	Assess the probability of risk event occurring	Assess the plausible impact of risk event occurring	Residual Risk Level	Risk Acceptance Criteria	Plan/Justification for Residual Risk	Risk Treatment Status	Describe the Remarks if any e.g.; acceptanc e criteria

- Residual Risk: Document the risks that exist even after the controls are taken into account and implemented effectively.
- Likelihood of residual risk: Determine the likelihood of the residual risk based on the residual risk as follows: Frequent / Possible / Rare. The definition of the likelihood ratings is as follows:

Likelihood	
The probability of risk occurring:	
RATING	POTENTIAL FOR RISK TO OCCUR
Frequent	Likely to occur several times a year
Possible	Possibly occurs once a year or 2 years
Rare	Possibly occurs once 5- 10 years

- Impact of residual risk: Determine the impact of the residual risk irrespective of the controls implemented as follows: Major / Moderate / Incidental. The definition of the impact ratings is as follows:

Consequences	
The potential outcome of a risk event that affects a firm's business objectives on the assumption that an event has occurred and the most probable consequence has resulted rather than the worst-case scenario.	
RATING	POTENTIAL FOR RISK TO OCCUR
Major	The loss of confidentiality, integrity, or availability could be expected to have a major adverse effect on operations, assets or individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a moderate adverse effect on operations, assets or individuals.
Incidental	Little/negligible impact on operations, assets or individuals with no legal consequences.

- Residual Risk: The value of residual risk is automatically calculated based on the likelihood and impact ratings.

$$\text{Risk Level (residual)} = \text{Likelihood} * \text{Consequence}$$

Risk Evaluation Criteria			
LIKELIHOOD		IMPACT/CONSEQUENCE	
	Incidental	Moderate	Major
Frequent	3	6	9
Possible	2	4	6
Rare	1	2	3

- Below table depicts the Risk Level based on likelihood and consequence of the risk :

Level of Risk		
The ranking assigned after considering the likelihood and consequence of a risk		
Risk Level	Activity	Range
High	Needs Action	7-9
Medium	Needs Attention / Improvement	4-6
Low	Monitoring Needed – Annually	1-3

*Range values are obtained from the risk evaluation criteria table.

- Risk Acceptance Criteria: The various reasons for accepting risk as defined as below:

Reason	Details
Budgetary / Financial	There will be financial constraints binding on the extent of implementation of security controls
Environmental	Environmental factors, such as space availability, climate conditions, natural and urban geography, may influence the selection of safeguards
Technological	Some measures are technically not feasible, e.g. incompatibility of hardware or software
Cultural	Sociological constraints on the implementation of safeguards may be specific to a country, a sector or an organization
Time	Not all safeguards can be implemented immediately. Some take a longer time to implement, some need to wait for a suitable opportunity, some are dependent on completion of other tasks

Reason	Details
Personnel	Required manpower may not be available immediately.
Legal	There could be legal constraints
Other	There may be different reasons other than those stated above for non-implementation

- Plan or justification of residual risk: The plan to resolve and reduce the residual risk effects should be documented.
- Risk treatment Status for residual risks : Based on the plan for managing the residual risks, the following could be the status for the treatment plan:
 1. Ongoing : Select if the treatment is a continuous activity
 2. Planned: Select if the treatment is planned and yet to be implemented.
 3. Implemented: Select if the treatment plan has been implemented and executed.
- Remarks (If any): Deviation to the process or risk acceptance criteria should be documented.

3. Maintenance of Risk Management Methodology

In view of the constant change of operating environment in terms of people, process and technology, management should ensure risk monitoring and compliance regime on an on-going basis to ascertain the performance and effectiveness of the risk management process. Further, improvements should be documented and implemented, as dictated by regular review of the ISMS and events that impact the risk management to ensure that the risk management methodology does not become obsolete.

Choice should conduct at least an annual review of risk management methodology, the risks identified, their assessment and treatment plans. CISO is responsible for the overall review and update of risk management methodology and risk assessment and treatment sheet. Individual owners are responsible to review and update the related risks and their treatment plans. The reviews should include adequacy and effectiveness with regard to any identified significant changes in Choice, changes in technology, changes in business objectives and processes, changes in identified threats and changes in legal and regulatory environment. Further, reviews should be performed whenever there is an incident.

4. References

1. Risk Management Template