Quick Heal Technologies Ltd

Risk Management Charter and Policy

Table of Contents

1.0 Introduction

Quick Heal Technologies Ltd ("QUICK HEAL") (Formerly Known as Quick Heal Technologies Pvt. Ltd.) is one of the leading IT security solutions company. Each Quick Heal product is designed to simplify IT security management across the length and depth of devices and on multiple platforms. They are customized to suit consumers, small businesses, Government establishments and corporate houses.

Over a span of 20 years the company's R&D has focused on computer and network security solutions. The current portfolio of cloud-based security and advanced machine learning enabled solutions stop threats, attacks and malicious traffic before it strikes. This considerably reduces the system resource usage. The security solutions are indigenously developed in India.

A number of practices and forms are adopted by the Management while taking decisions and monitoring performance, including functional and business review, which address current performance and future direction and changes thereto, as well as addressing potential risks. As a part of strengthening and institutionalising the decision making process and monitoring the exposures that are faced by QUICK HEAL, a formalised Risk Management System is being implemented on an Enterprise-Wide-Scale (ERM).

Managing Risk is a skill that is sought to be strengthened through this process and an effort at making decision making more consistent in a way that the business objectives are met most of the times. The ERM process seeks to provide greater confidence to the decision maker and thus enhance achievement of Objectives.

As a part of the Corporate Governance requirements under the Companies Act, 2013 and also under the Listing Agreement of the Stock Exchanges, there is a requirement for Public Listed Companies to have Risk Management Policy in place.

This document outlines the Charter – the purpose, authority and responsibility and the Policy as related to ERM.

2.0 Risk Management Charter

QUICK HEAL is committed to ensuring:

- Sustainable business growth,
- Safeguard of all STAKEHOLDER interests
- Minimal surprises in performance due to internal and external business environment changes and
- Adherence to applicable regulatory requirements
- Help business leaders and management decide on the rationale for either of;
    - Taking the risk
    - Safeguards / insurance to taking that risk (i.e. sharing it with others or avoiding it altogether)
    - Costs of such safeguards vis-à-vis upside / downside of accepting risks
    - Periodic review of the afore-stated positions

The Risk Management Charter establishes a formal framework of Enterprise Risk Management in Quick Heal Technologies Ltd and is the basis for ALL ERM related activities in the organisation.

This Charter complements and does not replace other existing compliance programs, such as control processes, financial and operational audits, ISO, quality systems, internal and external reviews, etc. This charter is built on globally established principles of sound risk management.

2.1 Applicability

This Charter is applicable from the date of its release and applies to whole of the company (which includes its subsidiaries), and includes all functions and departments.

2.2 Enterprise Risk Management Objective

The Objective of Enterprise Risk Management is superior achievement of business goals through:

- improved and consistent decision making taken by all in the organisation and
- a culture of thinking about the downside and upside of decision making based on judgment and data

In the process regulatory requirements for a Risk Management System and Policy are also sought to be complied.

To realize the risk management objective, the Company aims to ensure that:

- The identification and management of risk is integrated in day to day management of the business
- Risks are identified, assessed in the context of the measurable scales of Consequence and Likelihood, continuously monitored and managed to an acceptable level,
- The escalation of risk information is timely, accurate and complete, to support decision making at all management levels.

2.3 Risk Management Principles

The principles contained in the policy will be applied at both corporate and operational levels to all locations within the company. These are broadly divided in two parts viz. General Principles and Specific Principles.

2.3.1 General Principles

- All the risk management activities will be aligned to
    - the Vision and Mission Statement of the Company and of each function and branch
    - corporate aims, and organisational priorities of the company

- Risk analysis will form part of the Company`s strategic planning, business planning and investment/project appraisal procedures
- Managers and staff at all levels will have a responsibility to identify, evaluate and manage and/or report risks.
- Risks will be primarily managed by the business functions transacting the business which gives rise to risks
- The Company will foster a culture which provides for spreading best practice, lessons learnt, and expertise acquired from risk management activities across the company for benefit of the entire company.

2.3.2 Specific Principles

- Risk Management in the Company should be proactive and reasoned (and always forward looking). Corporate and operational risks should be identified, objectively assessed and actively managed.
- The aim is to anticipate, and where possible, avoid risks rather than dealing with their impact. However, for the same key areas where the likelihood of risk occurring is relatively small, but the impact on the Company is high, the Company may cover that risk by developing plans, e.g. Business Continuity Plans. This will allow the Company to contain the negative effect of unlikely events which might occur.
- In determining an appropriate response, the cost of control/risk management, and the upside / downside impact of risk occurring will be balanced with the costs of reducing risk. This means that the response will not be disproportionate to the impact or expected benefits.
- The Company recognizes that some risks can be managed by transferring them to a third party, for example by contracting out, hedging or possibly, by insurance.

2.3.3 Definitions

The risk management policy is formed around a common understanding of terminology used in this document.

Risk

The risk of direct or indirect loss or opportunity from internal process, people and systems, or from external events. It can also be defined as anticipated event or action that has a chance of occurring, which may result in positive or negative impact. In short, Risk is an event that can negatively impact the stated business plan of the Company. Positive surprises are also negative in the sense that this means the leadership does not have a proper handle on issues involved, and this can create credibility issues with customers and markets.

More specifically, Risk is the effect of uncertainty on the objectives. Risk is measured in terms of Consequences and Likelihood.

Consequence is the extent of an impact. Likelihood is the frequency of occurrence.

Risk has three primary components:
1. What happens – the Risk Incident;
2. Why it happens – the Source & Cause;
3. What is impacted – the Objectives.

To explain:
For each risk, there are questions the team needs to answer, in order to understand their incidence and the nature of risk. There are six parameters for which each risk needs to be tested for:
a. Would the risk be strategically important to bear for the organization (e.g. For a forex trader, assuming the volatility risk for a set of currencies would be essential to his calling, while for a business focused on providing software products, this would not be strategic to their earnings capability – however the risk of technology change is a risk the software company would use to create a sustainable business advantage)
b. What factors need to be considered to define the probability of risk occurring, and classifying this into a rating matrix capturing the level of probability for that risk?
c. What different ways could we measure the adverse impact of the risk, on earnings and cash flows of the company?
d. What returns could accrue if we bear the risk?

The next 2 questions are raised at the stage of Risk Analysis, Evaluation and Treatment when existing controls are reviewed -

a. What financial or non-financial instruments are available to the company to mitigate the risk, wherever possible?
b. What considerations need to be factored in while measuring the cost of mitigating risks thus.

'Control Systems'

Anything that is done to assist achieve QUICK HEAL's objectives is a 'control system', including:

- QUICK HEAL's culture and organization;
- Leadership and teamwork;
- Information systems;
- Policies, standards and procedures;
- Communication processes;
- Staff training and development;
- Performance targets, records, reports;
- Financial measurements and reports.

If control is not effective in managing identified risks, then risks are 'treated' by improving control.

Risk Management

The co-ordinated activities to direct and control an organisation with regard to risk. The systematic process of identifying, analysing, and responding to anticipated future events that have the potential to impact objectives.

Risk Analysis

The process of determining how often specified events may occur (likelihood) and the magnitude of their consequences (impact).

Risk Evaluation

The process of determining Risk Management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria, to generate a prioritized list of risk for further monitoring and management.

Risk Assessment

Risk assessment is the combined process of Risk Analysis and Risk Evaluation.

2.4 Structure

The Risk Management Structure, roles and responsibilities are set out in para 3

2.5 Risk Management Approach

The Risk Management Approach is explained in details in para 4

2.6 Documentation

Appropriate documentation at each stage of the risk management process should be followed. This framework provides a guide to documentation standards and how they are to be utilized.

The documentation will serve following purpose:

- Demonstrate that risk management process is conducted properly
- Provide evidence of systematic approach to risk identification and analysis,
- Provide a record of risks to support the development of database of the Company`s risks
- Provide risk treatment plans for approval and subsequent implementation
- Provide accountability for managing the risk identified
- Facilitate continuous monitoring and review
- Provide an audit trail and
- Share and communicate risk management information across Company.

The responsibility for documenting individual risks has been assigned to risk owners.

The key documents pertaining to the risk management process that needs to be maintained by the company are:

- Risk Management Charter and Policies
- Risk Register
  Containing list of all the risks that have been identified during the periodical review. It is the key document used to communicate the current status of all the known risks and is used for management control, reporting and reviews. The consolidated risk register is owned by the Risk Management Steering Committee (RMSC) and will be maintained by respective risk owners. The template of the Risk Register and Risk Treatment Plan is given in **Annexure 3 and Annexure 4.**
- Risk Management Report
  The report is to be placed before the Board of Directors for review and approval

2.7 Sign Off

The Risk Register and the Risk Management Report should be signed by the Chief Risk Officer.

3.0 Risk Management Organisation

The organisation structure for risk management is depicted through the flow chart below. Detailed noted on roles and responsibilities of each level follow.

3.1 Risk Management Steering Committee (RMSC)

Primary Functions

Risk Management Steering Committee is an excellent tool to make the business accountable for the identification, assessment, mitigation, and communication of risk. The committee oversees the risk management processes for company. The committee will:

- Provide risk management leadership for IT through the alignment of IT strategic objectives, and activities with enterprise strategic objectives and processes.
- Prioritize IT risk exposures and thresholds, and resolve resource allocation issues based on risk prioritization.
- Ensure optimal risk management through service target measurements.
- Ensure open communication between the IT department and the other functional departments so as to promote collaborative risk management.

A detailed note on the **Steering Committee** meeting is given in **Annexure 2.**

Agenda

The agenda of a typical RMSC meeting will include the following items:

1. Identify and review major risks throughout the organization.
2. Recommend an appropriate risk appetite or level of exposure.
3. Review the assessment of the impact and likelihood of identified risks.
4. Review the prioritized list of risks.
5. Create a mitigation plan to minimize risk impact and likelihood.
6. Review and communicate overall risk impact and risk management success.

Membership

- Chief Executive Officer
- Chief Technical Officer
- Chief Finance Officer
- Chief Risk Officer
- Chief Information Security Officer
- Head of IT
- Head of HR
- Additional Head of Business Unit

- Company Secretary

The Chief Information Security Officer (CISO) is the Chief Risk Officer.

All permanent members of the RMSC should be very familiar with the IT department's policies, procedures, and practices. As well, all permanent members should have the authority to make decisions, and take actions on behalf of the business unit they represent.

Operation and periodicity of meeting
The Chief Risk Officer will chair the RMSC. The Company Secretary will be responsible as the Secretary to the RMSC. The RMSC shall meet on quarterly basis or more frequently if required for urgent matters.

Mandate

- All proposals must follow a specific business case methodology as mandated by the RMSC. This methodology includes clear definitions of possible risk scenarios and events, and a thorough risk assessment, namely an impact/likelihood analysis, and clear calculation of potential costs to the business and cost to mitigate.
- The committee shall review all proposals for risk management. This includes proposals from within the IT department as well as proposals from other departments that have a significant IT component.
- All proposals must be formally presented in person to the RMSC by the business unit head.
- RMSC has the authority to reject any proposal which it deems as an insufficient attempt to manage risk, or which does not significantly contribute to the strategic goals of Company.
- At each meeting, the committee will receive progress reports on all previously approved proposals. The RMSC can recommend the termination of any service, which is not meeting its projected goals.

Deliverables
At a minimum, the RMSC will deliver:

- Annual assessment of risks
- Quarterly review of risks
- Quarterly updated Risk Register and Risk Profile (including mitigation plans)
- Reports required for the Board of Directors/Audit Committee.

3.2 Marketing Risk Management Committee (MRMC)

Primary Functions

The MRMC will coordinate the risk management initiative. Marketing risk is broadly classified into credit risk, market risk and operational risk. Risk Management is a methodology that helps managers makes best use of their available resources. The process consists of important steps like:

Identification of Risks
Analyzing the Risks
Evaluating the Risks
Monitor and Review
Mitigation of Risk

Membership
Standing membership of the MRMC will consist of the Country Manager, Business Controller, Regional Marketing Heads and Branch Managers.

All the functional heads and other senior personnel from the HO may be invited to participate in the meetings as required.

Operation and periodicity of meeting
Respected Country Manager will chair the MRMC who will select a designated person to act as the Secretary of the MRMC. As per define the MRMC meeting will be conducted simultaneously with **Business Review/Strategic Marketing** meeting on quarterly basis.

A detailed note on the **Business Review/Strategic Marketing** meeting is given in **Annexure 1.**

- There should be a good support from the Information Technology wing for creating an integrated system whereby an effective and efficient MIS would be an integral part of the risk management.
- There should be clear demarcation of functions and authority levels to ensure better internal control systems.
- An effective communication system coupled with the training programs.
- One of the risk mitigation measures is to setup appropriate limits. Inbuilt checking and balancing systems
- A periodical review and evaluation system should be in place.

Deliverables

- Annual assessment of risks
- Quarterly reviews of risks
- Quarterly updated Risk Register and Risk Profile (including mitigation plans)
- Reports required for the RMSC

The Country Manager as the chairperson of MRMC will represent all reports to management at the RMSC.

3.4 Corporate Risk Management Committee (CRMC)

The CRMC will coordinate the risk management initiative for the following departments/activities at the Corporate Office:

- Finance, Accounts and Taxation
- Legal and Regulatory Compliance
- Human Resource
- Administration

Membership

Standing membership of CRMC will consist of the departmental/functional heads and designated senior personnel at the Corporate.

Operation and periodicity of meeting

The CFO will chair the committee. The Company Secretary will be responsible as the Secretary to the CRMC. The CRMC shall meet on a quarterly basis or more frequently if required for urgent matters.

Other senior personnel may be invited to participate in the committee meetings as required.

Deliverables

At minimum, the CRMC will deliver:

- Annual assessment of risks
- Quarterly review of risks
- Quarterly updated Risk Register and Risk Profile (including mitigation plans)
- Reports required for RMSC

A representative from this Committee would be member of the RMSC on yearly rotational basis.

3.5 Chief Risk Officer

Chief Risk Officer (CRO)

The CRO would be member of RMSC and responsible as coordinator for risk management activity for entire company. The CRO would coordinate information flow between the RMSC and the Risk Owners. Also the CRO would liaise with the MRMC, R&D RMC and CRMC to coordinate flow of information between them.

3.6 Risk owners

Risk Owners will primarily be the Functional Heads and also those who are identified for specific risks. Role of the Risk Owners is to assess, review, monitor, and respond to risks, evaluate and validate the status of the risks and propose controls

The Risk Owner shall meet his team members every quarter (at least 15 days prior to meeting of committee) to discuss new risks added to the risk register during the quarter and review the implementation status of mitigation plans. Risks reassessed during the meeting of Risk Owners, shall be presented to MRMC, R&DRMC and CRMC for consolidation and reporting to the RMSC.

3.7 Roles and Responsibilities

The risk management roles and responsibilities will be as follows:

Roles	Responsibilities
Board of Directors	▪ Review and approve risk management and management reports ▪ Authorise risk management charter and policies ▪ Support risk management practices
Audit Committee	▪ Review adequacy and effectiveness of business risk management ▪ Review and approve (internal and external) audit plans ▪ Monitor business risk reporting
Risk Management Steering Committee (RMSC)	▪ Develop and maintain risk management charter and policies ▪ Advice business units on risk initiatives ▪ Spearhead risk management initiative within the company ▪ Monitoring emerging issues and share best practices ▪ Commission and oversee projects to define and implement risk mitigation strategies ▪ Improve risk management techniques and enhance awareness ▪ Set standards for risk documentation and monitoring ▪ Recommend training programs for staff with specific risk management responsibilities ▪ Assess and manage risk for corporate and company as a whole ▪ Review and approve the Risk Management report prepared by the CRO ▪ Report the Enterprise-Level Risk Matrix, Heat Map and Mitigation strategies periodically to the Audit Committee. Such periodicity will be set up in consultation with the Audit Committee.
Chief Risk Officer(CRO)	▪ Oversee execution of risk management strategies and policies ▪ Report to and update the RMSC on the risk management program ▪ Prepare Risk Management Report for the company as whole ▪ Monitor risk exposure versus limits as drawn by the RMSC ▪ Coordinate the risk management initiative for the company as whole as per the risk management charter and policies and directives of the RMSC. ▪ Responsible for giving directions to and coordinating with the heads of MRMC and CRMC
Secretary to RMSC	▪ Issue certificate of compliance based on the review of the quarterly risk management reports ▪ Responsible for ensuring that required documentation has been maintained and required sign offs have been obtained ▪ Maintain the reports of RMSC activities and meetings ▪ Ensuring the RMSC meetings are held as required ▪ Maintaining minutes of meetings held
Marketing Risk Management Committee (MRMC)	▪ Spearhead the risk management initiatives of the marketing and business development function at corporate ▪ Oversee project implementation of risk mitigation strategies ▪ Assess and manage risk for Marketing and Sales ▪ Escalate Risks to RMSC on the need basis ▪ Reporting periodically as specified by the RMSC
Secretary to MRMC	▪ Issue certificate of compliance based on the review if the quarterly risk management reports ▪ Responsible for ensuring that required documentation has been maintained and required sign offs have been obtained ▪ Maintain the reports of MRMC activities and meetings ▪ Ensuring the MRMC meetings are held as required ▪ Maintaining minutes of meetings held
Research and Product Development Risk Management	▪ Spearhead the risk management initiatives of the Research and Product Development function ▪ Oversee project implementation of risk mitigation strategies

Roles	Responsibilities
Committee (R&D RMC)	▪ Assess and manage risk for Research and Product Development ▪ Escalate Risks to RMSC on the need basis ▪ Reporting periodically as specified by the RMSC
Secretary to R&D RMC	▪ Issue certificate of compliance based on the review if the quarterly risk management reports ▪ Responsible for ensuring that required documentation has been maintained and required sign offs have been obtained ▪ Maintain the reports of MRMC activities and meetings ▪ Ensuring the R&DRMC meetings are held as required
Corporate Risk Management Committee (CRMC)	▪ Spearhead the risk management initiatives of the marketing and business development function at corporate ▪ Oversee project implementation of risk mitigation strategies ▪ Assess and manage risk for areas other than Marketing ▪ Escalate Risks to RMSC on the need basis ▪ Reporting periodically as specified by the RMSC
Secretary to CRMC	▪ Issue certificate of compliance based on the review if the quarterly risk management reports ▪ Responsible for ensuring that required documentation has been maintained and required sign offs have been obtained ▪ Maintain the reports of CRMC activities and meetings ▪ Ensuring the CRSC meetings are held as required ▪ Maintaining minutes of meetings held
Risk Owners	▪ Responsible for identifying risk ▪ Responsible for reassessing on periodic basis ▪ Responsible for preparing risk register and risk profile ▪ Suggest mitigation plans ▪ Responsible for managing risk by implementing mitigation plans
Employees	▪ Responsible for identifying risks ▪ Compliance with request from management in connection with application of this policy ▪ Exercise reasonable care to prevent loss, maximise opportunity and to ensure that operations, reputation and assets are adversely affected.

4.0 Risk management Process

4.1 Risk Identification and Reviews

Comprehensive risk identification using a well-structured systematic process is critical, because a potential risk not identified will be excluded from further analysis. Identification should include all risks whether or not they are under the control of the Company.

Each Risk Owner must monitor the risks faced by the function on a regular basis and more specifically on a quarterly basis assess the risks that they face as a group based on the defined objectives, internal and external context realities and the Stakeholder objectives. It will not be limited to a review of risks already identified but will include a review of the changes in the environment. This review should include identification for all significant areas. Workshops or brainstorming sessions may be conducted amongst the group to identify new risks that may have emerged over a period of time. This review will include a documented analysis of the reasons for all successes and failures vis-à-vis the Objectives in the daily working or projects undertaken and identifying the learning for the future.

All identified risk should be updated in risk register. Risk register should be periodically reviewed by the respective risk owners to ensure pertinence of the risk listed. Risks that are no longer relevant should be closed appropriately.

The CRO and heads of the MRMC and CRMC should ensure that risk register are reviewed and updated quarterly. They are also responsible for ensuring that the learning is from the Success/Failure analysis is documented for easy reference.

4.2 Risk Assessment

The risk will be assessed on qualitative two fold criteria. The two components of risk assessment are (a) the likelihood of occurrence of the risk event, and (b) the magnitude of impact if the risk event occurs. **The combination of likelihood of occurrence and magnitude of impact provides the risk level**. Where needed, guidance, as provided in **Annexure 4**, may be used for this qualitative assessment.

The magnitude of the impact of an event, should it occur and the likelihood of the event and its associated consequences, are assessed in 2 stages –

1. Inherent Risk – Assessment before considering any action taken to mitigate the consequence or likelihood of risk.
2. Residual or Controlled Risk – Assessment in the context of the existing controls that mitigate the consequence or likelihood of Risk.

The impact and likelihood may be determined using statistical analysis and calculations. Alternatively, where no past data are available, subjective estimates may be made which reflect an employees, or group`s degree of belief that a particular event or outcome will occur.

In determining what constitutes a given level of risk the following scale is to be used for likelihood:

Levels	**Description**
5	Almost Certain
4	Likely
3	Moderately Likely

Levels	**Description**
2	Unlikely
1	Rare

In determining what constitutes a given level of risk the following scale is to be used for impact:

Levels	**Description**
5	Critical
4	Major
3	Moderate

Levels	**Description**
2	Minor
1	Insignificant

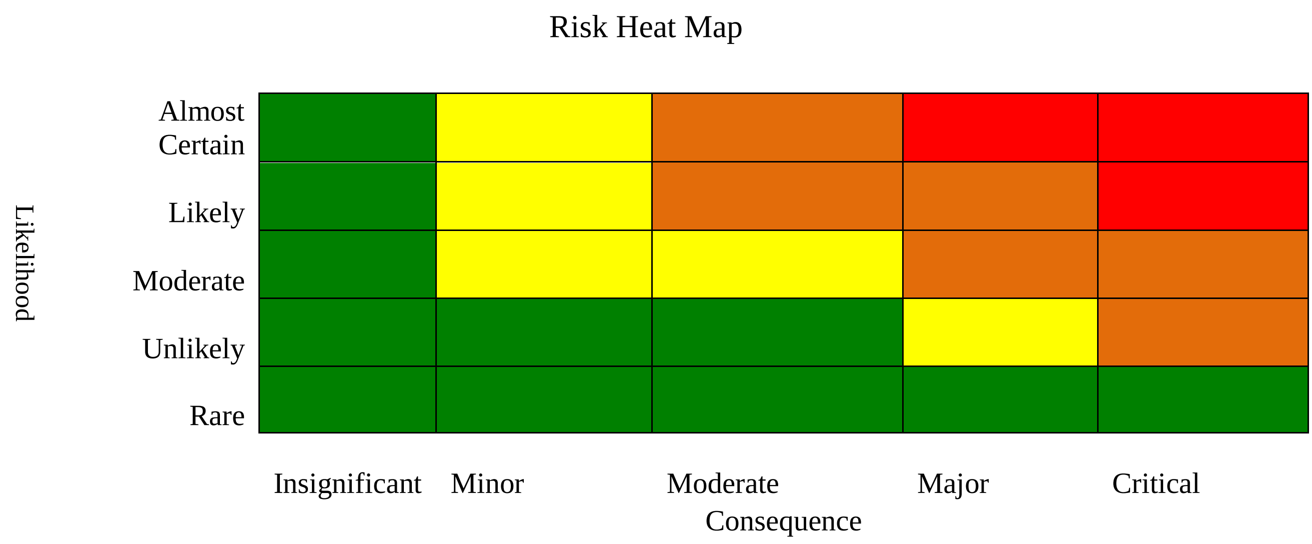
Over a period of time, endeavour should be made to assess the risk on quantitative basis. Assumptions should be defined where financial impact in Rupee terms is calculated. RMSC should review and revise the assumption based on latest budgets, cost records, financials and forcasts for present/future of business and industry.

Precise quantification of the Rupee value impact of risks is sometimes impracticable, since the ultimate cost would depend on significant number of variables. Where values can be assigned it is necessary to look at the above effects over future time period rather than that particular financial year.

4.3 Risk Evaluation

Impact and Likelihood are combined to produce a level of risk. For each risk, the score for likelihood and impact should be multiplied to arrive at combined score. The risk classified into one of the four zones based on combined score.

- Risks and Likelihood within red zone are considered “Extreme” and require immediate action plans to close a significant control gap. (score 20 or above)
- Risks and Likelihood within amber zone are considered “High” and require short term action plans to close a significant control gap. (score 12 or above and below 20)
- Risk that score within the yellow zone are considered “cautionary” where action steps to develop or enhance existing controls is also needed. (score 6 or above and below 12)
- Risks that score within the green zone are considered “acceptable” or in control. (Average scores less than 6)



The objective is to define the risk treatment and monitoring strategies for appropriate attention and effective utilization of Company resources in managing risks.

The output of risk evaluation is prioritized list of risks for further action. This should be documented in a “Risk Assessment Report. The report should be signed by the CRO and the Head of MRMC, or CRMC as applicable.

4.4 Risk Treatment/Action Plan

Risk Treatment involves identifying the range of options for treating risk, assessing those options, preparing risk management plans and implementing them. Treatment options may include:

- Accepting the risk level within the established criteria
- Transferring the risk to other parties e.g. insurance
- Avoiding the risk by hedging/adopting safer practices or policies and
- Reducing the likelihood of occurrence and/or consequences of risk event.

Action plans need to be time bound and responsibility driven to facilitate future status monitoring. Mitigating practices and controls shall include determining policies, procedure, practices and processes in place and additional resource allocation what will ensure that existing level of risks is brought down to an acceptable level. In many cases significant risk may still exist after mitigation of risk level through the risk treatment process. These residual risks will need to be monitored.

4.5 Escalation of Risks

It is critical to institute an effective system of escalation which ensures that specific issues are promptly communicated and followed up appropriately. Every employee of the Company has responsibility of identifying and escalating the risks to appropriate levels within the Company. This involves an assessment of controls to mitigate the risks. In case controls are not performing as designed or the proportion of deviation is high there is a need to reassess the Risk and also put in place a corrective program. The CRO and the Committee heads will determine whether the risk needs immediate escalation to next level or it can wait till subsequent periodic review.

5.0 Reporting

A Risk Management report should be prepared by the secretaries to the MRMC and CRMC respectively. Report for the whole company should be prepared by CRO of the RMSC. The report prepared should be placed before the Board. The frequency of the review and reporting of the risk management is given below:

5.1 Review and Reporting Cycle

Functions	Frequencies	Dates
Establishment of Risk Management Process	Once	As approved
Updating Risk Register	As and when risks are identified at least once in quarter	June, September, December, March
Risk Assessment	Quarterly	June, September, December, March
Risk Management Report	Quarterly	June, September, December, March

Annexure 1
Business Review/Strategic Marketing –cum- MRMC Meeting

Primary Functions
Planning your strategic marketing starts with research that focuses on identifying your prime customers, their demographics and buying habits. The team will first review past sales performance and marketing activities.

Followed by initiating planning future strategic marketing and business development. All functional heads will also act as MRMC (Marketing Risk Management Committee) to identify and manage specific marketing risks as per the MRMC policy.

Membership
The team will consist of the respected vertical Country Managers (Marketing), The Business Controller, Regional Marketing Heads and Branch Managers. The Country Manager will plan this meeting, prepare an agenda in advance and send a meeting invite to the respective marketing team.

Operation and periodicity of meeting
The Country Manager will chair the meeting who will select a designated person to act as the Secretary to document the minutes of meeting. The team shall meet on quarterly basis or more frequently if required for urgent matters.

Regional Marketing Heads shall meet his team members every month to review sales performance and to discuss new risks added with mitigation plan. Regional Marketing Heads shall present to the respected Country Manager a consolidated report during quarterly meetings.

All the functional heads and other senior personnel from the HO may be invited to participate in the quartely meetings as required.

Strategic marketing planning meetings are what you do before you do tactical planning. In other words, strategic marketing is the "why" of your planning, and tactical marketing is the "how" that delivers the goals of your strategy. Marketing risk is broadly classified into credit risk, market risk and operational risk.

Team will also take notes as minutes of the meeting, and be sure to start on time.

Begin the meeting by objectives and how long you expect the meeting to last. This one gesture will go a long way toward communicating that you are disciplined and respect other people's time.

Identify the actions that must be taken to achieve your marketing tactics and an effective risk management, the person responsible for implementing each tactic and the deadlines.

Ascertain that everybody understands his or her responsibilities and deadlines, in successfully implementing the marketing plan.

Open the floor for questions and answer.

Conclude the meeting by reviewing the appropriate action steps before setting a date for your next meeting.

Annexure 2
Steering Committee–cum- Risk Management Meeting

Primary Functions

In Information Technology Product Company, the job of a steering committee is to make sure every software development strategy towards existing product feature enhancement or new product development, Product sales and marketing strategy supports business goals and objective. The steering committee is often responsible for creating working groups and choosing the right experts. The committee will also monitor and review each activity.

The Steering Committee provides a stabilizing influence so organizational concepts and directions are established and maintained with a visionary view. The Steering Committee provides insight on long-term strategies in support of legislative mandates. Members of the Steering Committee ensure business objective are adequately addressed and the product development and marketing activities remains under control. In practice performing the following functions carries out these responsibilities.

- Setting objective of an Steering committee
- Building a business plan
- Monitoring progress towards goals
- Providing assistance to all activities when required.
- Making the business accountable for the identification, assessment, mitigation, and communication of risk.
- Controlling scope as emergent issues force changes to be considered, ensuring that scope aligns with the agreed business requirements.
- Controlling scope, resolving conflicts / disputes and minimize risk.

Membership

The team will consist of the Chief Execitive Officer, Chief Technical Officer, Chief Finance Officer, Chief Risk Officer, Sr. Vice President Sales & Marketing and Sr. Vice President Business Logic. The Sr. VP's will plan this meeting, prepare an agenda in advance and send a meeting invite to committee members.

Operation and periodicity of meeting

Sr VP (Business Logic) will chair the SC meeting who will select a designated person to act as the Secretary to document the minutes of meeting. The SC shall meeting on quarterly basis or more frequently if required for urgent matters. The Team will follow modified Rules of Order in the conduct of meetings, motions, discussion and voting.

Approval Responsibilities

The Steering Committee is responsible for approving major elements such as

- Prioritization of product objectives and outcomes as identifying business
- Deliverables as identified in the project scope.
- Budget, ensuring that effort, expenditures and changes are appropriate to stakeholder expectations.
- Risk management strategies, ensuring that strategies to address potential threats to the project's success have been identified, estimated and approved, and that the threats are regularly re-assessed.
- Project management and quality assurance practices.

Role of a Steering Committee member

It is intended that the Steering Committee leverage the experiences, expertise, and insight of key individuals at organizations committed to building professionalism in product and business management. CXO are not directly responsible for managing project activities, but provide support and guidance for those who do.

Understand the strategic implications and outcomes of initiatives being pursued;

- Appreciate the significance for some major stakeholders and represent their interests;
- Be genuinely interested in the initiative and be an advocate for broad support for the outcomes.
- Have a broad understanding for approach being adopted by key team owners.

In practice, this means they:

- Review the status of the R&D and sales;
- Ensure the outputs meet the requirements of the business owners and key stakeholders;
- Help balance conflicting priorities and resources;
- Provide guidance to the teams;
- Check adherence of all activities to standards of best practice both within the organization and in a wider context;
- Report on progress to high-level management.

Agenda

Planning your business strategy starts with research that focuses on identifying your prime customers, their demographics and buying habits. The next step is a look at your current product mix and figure out what products and services are best suited to that target customer market, as well as new products and services to develop.

Review current product development status and market demand.

Same team will also act as RMSC members to identify and manage business risks as per the RMSC policy (Risk Management Steering Committee).

Introductory Items such as:

- Minutes from last meeting
- Review of actions arising from previous Steering Committee meetings.

Review R&D Status

- Overall Status
  - Scope status
  - Schedule status
  - Budget status
  - Reason for deviation if any.
- New issues arising since the last Team meeting
- Review and approval of project change orders
- Budget
- Milestone review
- Formal acceptance of deliverables
- Accomplishments against last meeting's plans
- Outstanding issues, open points, project conflicts
- Specific requests for assistance of the Steering Committee

Consideration of other relevant items.

Review and summarize new actions from this meeting

Annexure 3 - Template for Risk Register

Section 1												
					Inherent		Residual					
Sr. No.	Risk	Contributory Factors	Control	Control Effectiveness	Consequence	Likelihood	Consequence	Likelihood	Risk Score	Risk Level	Objectives	Risk Owner

Section 2						
Risk ID No.	Action Planned	Resource/ Capital Allocation	Responsibility	Completion Date	Remark	Sign Off

Quick Heal
Security Simplified

Annexure 4 – Risk Treatement Plan

Proposed Risk Treatment Actions				
Sr. No.	**Description**	**Target Dates**	**Status**	**Remark**
Sr. No.	**Resource Requirements**		**Responsibility**	**Budgeted Amount**
1				
2				
3				
4				
	Risk Owner			**Secretary - CRMC/R&DRMC**

NOTE: For completion of Risk treatment actions, the overall responsibility lies with respective Risk Owner

Calculations:

Assumptions:

Quick Heal
Security Simplified

Annexure 5 - Risk Measurement Matrix – Impacts

Value at Risk \ Rating	Critical (5)	Major (4)	Moderate (3)	Minor(2)	Insignificant (1)
Financial – Operating Profit	More than Rs. 5 lacs	Rs. 2 lacs to Rs. 5 lacs	Rs. 1 to Rs. 2 lacs	Rs. 0.50 lacs to Rs. 1 lac	Below Rs. 0.50 lacs
Financial – Cash Flow	More than Rs. 1 Crore	Rs. 50 lacs to Rs. 1 Crore	Rs. 25 lacs to Rs. 50 lacs	Rs. 10 lacs to Rs. 25 lacs	Below Rs. 10 lacs
Financial - Turnover	More than Rs. 5 Crores	Rs. 3 Crores to Rs. 5 Crores	Rs. 1 Crore to Rs. 3 Crores	Rs. 50 lacs to Rs. 1 Crore	Below Rs. 50 lacs
Regulatory – Legal Cases	Notices with Criminal Implications to Directors/Officers and/or Legal Case with critical impact on operating profits or Fines	Legal Case which has the potential of culminating in Criminal charges being made on Directors/Officers or major impact on operating profits or fines	Legal Case with Moderate to Critical Level of Fines or Financial impact on operating profits	Legal Case with minor fines or financial impact on operating profits	Minor breaches by staff members
Regulatory - Fines	More than Rs. 5 lacs	Rs. 0.25 lacs to Rs. 5 lacs	Rs. 0.10 lacs to Rs. 0.25 lacs	Rs. 0.02 lacs to Rs. 0.10 lacs	Below Rs. 0.02 lacs
Business Disruption	More than 36 hours	12 hours to 36 hours	6 Hours to 12 hours	2 Hours to 6 Hours	Below 2 hours
Sales & Marketing – Market Share	10%	7.50 % to 10%	5 % to 7.50 %	2 % to 5%	Below 2%
Reputation - General	Local/regional Media coverage (TV, News paper etc.) with serious negative impact.	5 or more incidences of malpractices/ quality issues etc. in a 12 month period	3 to 5 incidences of malpractices/quality issues etc.	2 to 3 incidence of malpractices/quality issues etc.	1 incidence of malpractices/quality issues etc.

Value at Risk \ Rating	Critical (5)	Major (4)	Moderate (3)	Minor(2)	Insignificant (1)
Reputation – Business Partners		Not Meeting Committed Terms of Business between 15% and 25% of the instances	Meeting Committed Terms of Business between 5% and 15% of the instances	Not Meeting Committed Terms of Business between 1% and 5% of the instance	Not Meeting Committed Terms of Business below 1%
Financial Reporting - Misstatement	More than Rs. 10 Crores	Rs. 7.50 Crores to Rs. 10 Crores	Rs. 5 Crores to Rs. 7.50 Crores	Rs. 2.50 Crores to Rs. 5 Crores	Below Rs. 2 Crores

Risk Assessment Matrix - Likelihood

Rating		**Occurrence**	**Probability**
Almost Certain	**5**	Happens once in week in Quick Heal or in the industry	Within 12 months
Likely	**4**	Happens once in month or occasionally in Quick Heal or in the industry	1 Years to less than 2 years
Moderate	**3**	Happen once in year in Quick Heal and in industry at global level	2 Years to less than 5 years
Unlikely	**2**	Happens once in 2 years in some units of the industry	5 Years to less than 10years
Rare	**1**	Happens in decade any where in the world in any industry	10 years or greater