MANNAI
CORPORATION

RISK MANAGEMENT PROCEDURE

Version No.	Implemented by	Revision / adoption date	Approved by	Reasons
1 (Current Version)	- Risk Manager - Management	27 Feb 2020	- Management - Audit Committee - Board of Directors	- QFMA Corporate Governance Code. - Documentation of Mannai Risk Management Framework.

Table of Contents

Introduction

All activities of an organization involve risk. Such risks include strategic, operational, financial, technological and socio-political risks that could impact the organization's business goals and objectives and affect the continued existence of the organization. Effective endurance requires identification and evaluation of the credible risks, integration of internal controls to manage risk, and strategic mitigation of unacceptable risks to ensure they are appropriately managed. An effective risk management process allows the implementation of mitigation measures to prevent adverse events from occurring and to plan for effective response where mitigation measures are unsuccessful.

The finite availability of resources for risk mitigation measures also requires a prioritization process based on the severity and likelihood of impact. Management is accountable for the provision of such resources and is an integral part of the risk management process via regular evaluations of risk sources and risk reduction measures.

This procedure document describes the mandatory requirements to achieve effective risk management and is implemented in accordance with the Company's corporate governance system.

1. Purpose & Scope

1.1. The purpose of this risk management procedure is to establish a framework to integrate the process for managing risk into overall governance, values, and culture in line with strategic and operational objectives. The risk management approach will aim to achieve a balance between maximising opportunities and minimising threats.

1.2. These procedures establishes roles and responsibilities for identifying, evaluating, and communicating risks as well as other critical activities needed for an effective risk management approach.

1.3. These procedures apply to all activities and employees. Both internal and external risks and impacts are subject to this procedure.

2. Definitions

Key Word	Definition
Risk	Potential future event that, if it occurs, will have an impact on achieving the business objectives, either positively or negatively.
Enterprise Risk Management	The process of identifying and analysing risk from an integrated, companywide perspective, as a basis for determining priorities for the application of risk responses.
Risk Management	The process of risk identification, risk assessment, risk prioritization, risk response and risk management and control.
Issue (e.g. Business deficiency)	An actual, known problem that must be managed (100% probability of occurrence).
Threat	Unfavourable condition or situation that can lead to a risk with a negative consequence.

Opportunity	Favourable condition or situation that can lead to risk with a positive consequence.
Uncertainty	A risk that cannot be quantified in terms of impact and probability. They are unknown due to inherent lack of knowledge or ambiguity (i.e. weather, force majeure, subsurface, etc.)
Risk Register	A body of information listing all the risks identified for our business, explaining the nature of each risk and recording information relevant to its assessment and management.
Risk Response	Action to eliminate, reduce or maximise (for opportunities) the probability of the risk arising, and/ or to eliminate, reduce or maximise (for opportunities) the significance of its impact if it does arise. Assign ownership to manage and control the risk.
Risk Identification	Determines which risks might affect the business and documenting their characteristics. Tools used for the identification of risks include brainstorming, checklists, and historical information.
Probability	Likelihood of occurrence of an identified risk.
Potential Impact	The impact of a risk on a business objective.
Probability & Impact Matrix	A Matrix also called a **Heat Map,** on which we can plot risks based on their probability and impact. Where these plot, we can determine if the risk is critical, important, significant, or unrated. The risks that plot in the highest probability/impact area are called "hot or critical" risks.
Qualitative Risk Analysis	The process of prioritizing risks for subsequent further analysis. The process assigns a probability of the risk occurring and the impact the risk is expected to have on the business. The combination of probability and impact is plotted on the **Probability Impact Matrix** to determine the priority of the risk.
Quantitative Risk Analysis	The process of numerically analysing risk information. This process provides the detail on the specific effects a risk or risk response will have on business objectives.
Risk Acceptance	A response where the team decides not to actively manage the risk.
Risk Allocation	Placing the responsibility for a risk to a party through a contract/ agreement.
Risk Assessment	A component of risk management that bridges risk identification and risk analysis in support of risk allocation
Risk Avoidance	A risk response where the team alters the plan so the risk is eliminated. Generally, risk avoidance involves relaxing one or more requirement of the business.
Risk Mitigation	A risk response that seeks to reduce the probability of occurrence or impact of a risk to an acceptable threshold.
Risk Transfer	A risk response planning technique that shifts the impact of negative risk/threat to a third party, together with ownership of the response (e.g. insurance)
Risk Owner	A person that is assigned to a specific risk. This person understands the risk and can take ownership for preparing information to further assess the risk and/or activate a risk response strategy.

3. Risk Ownership

All risk must have an identified individual as a risk owner based on their knowledge, job function and authority. Without a risk owner the risk will not be managed. It may be difficult to assign a risk owner to all risks, but all critical and important risks must have an assigned risk owner. Categorization allows the risk to be understood either based on its root cause, area of impact, or, other attributes and aligned with the most appropriate risk owner.

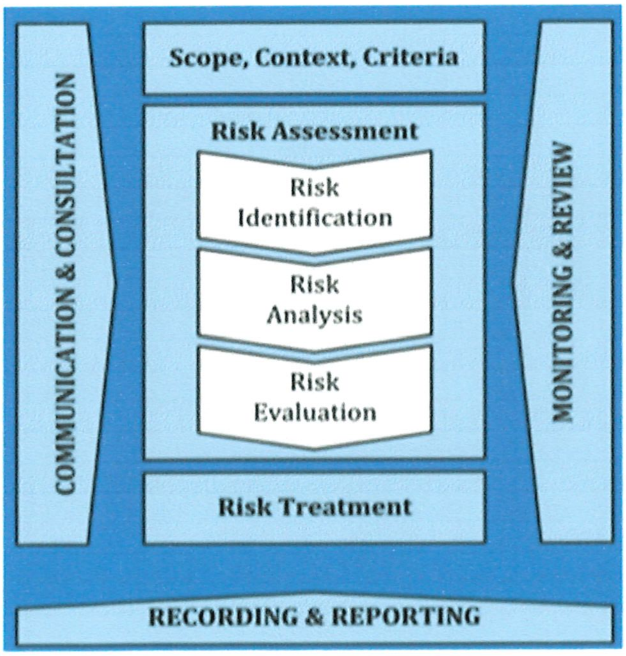
The risk owner is not necessarily the person who identified the risk. The risk owner would have understanding of the risk, would be able to determine what options are feasible for managing the risk, and whether the information that is provided is appropriate and sensible. Because the risk owner's knowledge is aligned with the risk attributes, the risk owner collects all the information, interprets it, and advises the Risk Manager on the risk situation and possible/ preferred options.

4. Enterprise Risk Management Process

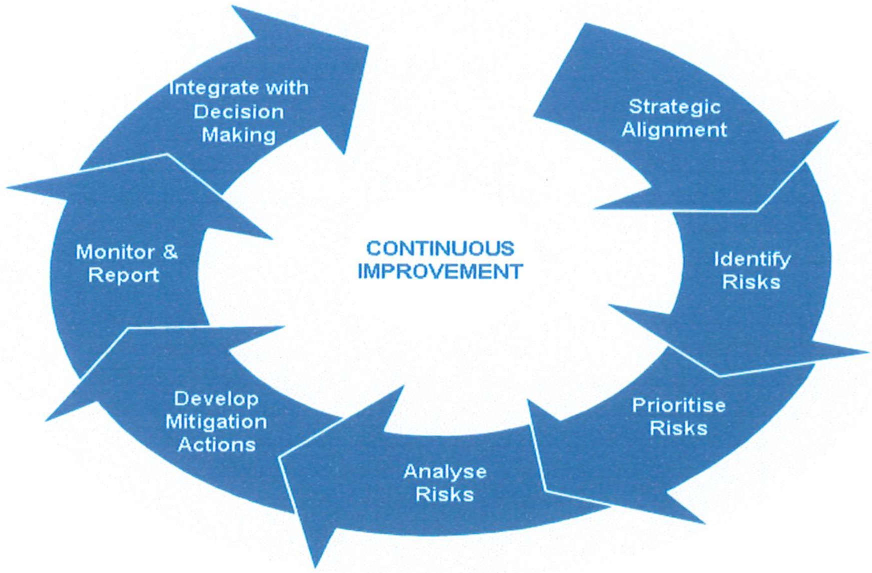
The cornerstone of Enterprise Risk Management (ERM) is to protect and assist in the achievement of corporate strategy and objectives, therefore it is critical that Risk Management is incorporated into existing processes to develop and manage corporate strategies and objectives, which serve as the foundation for all Risk Management activities. The ERM process is initiated from the development of the corporate objectives. These corporate objectives are developed at a strategic level and cascaded down through the organization as operational objectives and KPIs to individual employees.

Risks will be managed according to the Risk Management Framework which is based on the ISO 31000 Risk Management Process.

ISO 31000 Risk Management Process



Effective Risk Management Diagram



4.1 Identification

Risk identification is the first major component of best practice risk management. The purpose of risk identification is to gain a full understanding of any risk the organisation faces which might create, prevent, accelerate or delay the achievement of Company's objectives.

Mannai Corporation's Approach to Risk Identification

Risk identification is an ongoing and regular process to ensure new and emerging risks are addressed and incorporated within the risk management process. Current and possible forthcoming risks / issues are identified at both business unit / divisional levels as well as at a corporate level.

Mannai Corporation's Risk Register (the template is provided in Appendix A) is the main tool used to record the risk identification process and every risk identification session should begin with a review of the existing risk register.
The questions to ask are:

- Is there a risk to the Company that is not recorded in the risk register?
- Is there anything happening to the Company in the near future that could give rise to an emerging risk?
- Are there any risks recorded in the risk register that are no longer a risk to the Company?

There are a variety of techniques and methodologies that can be used to identify risks:

- Previous losses: these should be reviewed to identify the common causes which will allow related risks to be considered;
- Brainstorming: this brings together a number of people who all have differing perceptions of risk and the potential consequences if those risks were to materialise;
- Questionnaires: these can be used to capture a wide range of perceptions from a large group of people in a relatively short timescale; and
- Interviews: interviews provide the opportunity to explore potential risks in more detail, including the causes and consequences should they materialise.

For each risk identified the following information needs to be recorded in the risk register:

- Risk description: a short articulation of the risk
- Risk cause: the proximate cause(s) of the risk;
- Risk consequence: the consequence(s) to the Company should the risk materialise; and
- Risk category: a collection or group of risk types with a common denominator.

Risk Categorisation

Some risks will cross a number of categories and a common sense approach is to assign to the most relevant category. Categorising risks enables a more in-depth analysis of Company's risk profile. To ensure the risk identification exercise considers the spectrum of risks that can impact the organisation, Mannai Corporation considers risks across a number of different categories:

Risk Classification	Categories
Environment: risk arises when there are external forces that can affect a company's performance, or make its choices regarding its strategies, operations, customer and supplier relationships, organizational structure or financing obsolete or ineffective. These forces are outside management's ability to control.	Competitor Risk, Customer Wants Risk, Technological Innovation Risk, Sensitivity Risk, Shareholder Expectations Risk, Capital Availability Risk, Legal / Regulatory Risk , Sovereign/Political Risk, Financial Markets Risk, Catastrophic Loss Risk.
Governance: Risk that the organization's governance processes do not comply with legal and regulatory requirements or stakeholder expectations.	Organizational Culture Risk, Ethical Behaviour Risk, Board Effectiveness Risk, Succession Planning Risk.
Reputational: Potential for negative publicity, public perception or uncontrollable events to have an adverse impact on a company's reputation.	Image and Branding Risk, Stakeholder Relations Risk.
Operational: risks resulting from inadequate or failed internal processes or systems.	Customer Satisfaction Risk, Human Resources Risk, Knowledge Capital Risk, Product Development Risk, Efficiency Risk, Capacity Risk, Scalability Risk, Performance Gap Risk, Cycle Time Risk, Sourcing Risk, Channel Effectiveness Risk, Partnering Risk, Compliance Risk, Business Interruption Risk, Product/Service Failure Risk, Environmental Risk, Health and Safety Risk, Brand Erosion Risk, Planning Risk.
Empowerment Risk: The risk that managers and employees are not properly lead, do not know what to do (or how to do it) when they need to do it, exceed the boundaries of their defined authorities, do not have the resources, training and tools necessary to make effective decisions or are given incentives to do the wrong thing.	Strategic Risk, Leadership Risk, Authority/Limit Risk, Outsourcing Risk, Performance Incentives Risk, Change Readiness Risk, Communications Risk.

Information Technology Risk: Risk that the information technologies used in the business are not efficiently and effectively supporting the current and future needs of the business or threaten the company's ability to sustain the operation of critical business processes.	Integrity Risk, Access Risk, Availability Risk, Infrastructure Risk.
Integrity Risk: Risk of management fraud, employee fraud, and illegal and unauthorized acts, any or all of which could lead to reputation degradation in the marketplace or even financial loss.	Management Fraud Risk, Employee Fraud and Third Party Fraud Risk, Illegal Acts Risk, Unauthorized Use Risk.
Financial Risk: Risk that Company fails to provide adequate liquidity to meet its liabilities or meet financial risks in a manner that is inconsistent with its objectives. These risks manifest in a macro or micro economic way.	Price Risk, Interest Rate Risk, Currency Risk, Equity Risk, Commodity Risk, Financial Instrument Risk, Liquidity Risk, Cash Flow Risk, Opportunity Cost Risk, Concentration Risk, Credit Risk, Default Risk, Settlement Risk, Collateral Risk, Reporting Risk.

4.2Analysis

The analysis phase evaluates the inherent level of the risks, their negative consequences and the likelihood that those consequences may occur in the absence of suitable controls. The main objective of risk analysis is to assess qualitatively and when required quantitatively the level of risk.

To measure the consequences and likelihood following the criteria defined in the risk matrix, different techniques are used and may include statistical analysis and calculations. However, if there is no reliable or relevant past data available, subjective estimates may be used based on the knowledge and experience of concerned risk owner and by having brainstorming sessions to decide the possible levels of impact and likelihood which are then mapped onto the risk matrix to establish the *level of risk* of the identified event or risk scenario.

4.3 Evaluate

The risk matrix, used to evaluate the risk, provides a mechanism to rate, rank and prioritize risks based on rating for better allocation of resources to address high level risks.

Risk Management Matrix provides the required parameters to be used for the assessment of identified risks. The risk rating scale is based on the principle that a risk has two primary dimensions:

- Impact (Consequence): a risk, by its very nature, has a negative impact, and is the result or effect on an event. However the size of the impact varies in terms of cost and other related critical factors.
- Probability (Likelihood): the probability of an event happening / occurring over a 12-month period. Defined probability criteria shall be used to determine the probability level.

The mapping of the impact and likelihood of a risk event using the risk matrix *(without taking into account controls)* defines the Inherent risk rating of that particular event.

Definitions of Risk Ratings

Risk Rating	Definition
Negligible	Risk is of low significance. No immediate action required other than to monitor area for improvement.
Minor	Area for concern, a situation which if not addressed has potential to cause harm in the mid-long term / short term.
Major	A situation which if not immediately addressed will cause harm in short term. Prioritized action required. If no action taken, strategic objectives may be in jeopardy.
Critical	The organization will suffer severe bottom line impact in the long term. Prioritized action required. If no action is taken, the organization may suffer irrecoverably.
Catastrophic	The organization will suffer severe bottom line impact in the Short term. Immediate action required. If no action is taken, the organization will suffer irrecoverably.

4.4 Treatment

Risk Treatment strategies

Treatment strategy	Description
Terminate (Avoid)	Risk Rating is at a level with which the organization is uncomfortable, and the mitigation measures necessary are either impractical or unfeasible. Risks that are not acceptable and should be eliminated. Such risks shall be avoided as these are outside the tolerance level of department / organization and are thus not worth the risk.
Treat (Mitigate)	Implement mitigation measures to reduce either the probability of a risk event or its impacts, or both, allocate resources if necessary. Controls need to be developed and applied to bring the risk down to an acceptable level.
Transfer	On occasions when the level of risk is uncomfortable for the organization, but there are valid reasons not to directly treat the risk (e.g. cost / capability), the decision may be made to transfer the risk to a third party (contractor / insurance). The third party then owns the risk and is responsible for managing it. Taking out an insurance policy is a common way to transfer risks that have low Likelihood, but extremely high Severity.
Tolerate (Accept)	If the risk does not impact the current objectives and/or if the current level of control or Risk Rating is at a level with which the risk owner or organization is comfortable, the decision may be made to do nothing. There are no additional controls enhancement required. However, these risks are regularly reviewed to ensure that initial acceptance rationale is still valid. There are two types of acceptance, passive and active acceptance. **Passive acceptance** means no plans are made. The organization is willing to accept the consequences of the risk should it occur. **Active acceptance** might include developing contingency reserves to deal with risks should they occur.

Four strategies exist to deal with opportunities / risks that might present themselves. The Accept / Tolerate strategy has already been covered, the remaining strategies are as follows:

Opportunity treatment Strategies

Treatment strategy	Description
Exploit	Exploiting a risk event, is when the organization is looking for opportunities for positive impacts. This is the strategy of choice when Company wants to make certain that identified positive opportunities will occur in the business or project.
Enhance	The enhance strategy closely watches the probability or impact of the risk event to assure that the organization realizes the benefits. This entails watching for and emphasizing opportunities / risk triggers and identifying the root causes to help enhance impacts or probability.
Share	The share strategy is similar to transferring because it will assign the opportunities / risk to a third-party owner who is best able to bring the opportunity i.e. forming a joint venture.

The treatment strategy needs to be carefully studied before taking the decision to apply it.

Key Considerations for risk treatment strategy

Factors	Description
Impacts on risk	For each treatment strategy, predicted level of risk should be calculated considering the impact of adding the new control. Treatment strategy which reduces the level of risk to an acceptable level, should be considered.
Cost benefit analysis	An option may appear to be the best option to mitigate the risk, but the cost of implementation may be prohibitive. The selected strategy shall provide a balance between the incurred costs against the benefits derived.
Compatibility with objectives	The treatment strategy should be compatible with the overall objectives of the organization. Other strategies not in-line with organization objective should not be considered.

After consideration of all relevant factors, as well as consulting with any subject matter experts or particularly experienced members of the department, the risk owner shall make a decision on the treatment strategy.

The treatment options are implemented as controls against the identified risk. Once these required controls are identified and selected for implementation, they should be assembled into risk treatment plans (control implementation plan). Treatment plans should at the minimum record the following information:

- Proposed implementation plan and objective.
- Implementation responsibilities.
- Implementation time frame.
- Expected results of plan (in terms of risk consequence and / or likelihood reduction).
- Monitoring and review details.
- Include mechanisms for assessing and monitoring treatment effectiveness against treatment objectives; and
- Processes for monitoring treatment plan progress against implementation milestones.

The successful implementation of the risk treatment plan requires an effective management and communication plan. The risk owner is responsible for implementation of controls and recommending additional actions which shall result in improvement of existing controls or development of new controls.

After treatment, the residual risk shall be evaluated and a decision should be taken whether to retain this risk or repeat the risk treatment process. Residual risk is the level of risk remaining after risk treatment.

4.5 Risk Monitoring and Review

An effective monitoring process shall be implemented to adequately manage risk by promptly, detecting and highlighting deficiencies to reduce the potential likelihood and consequences of a risk materializing. All employees should be informed of the need to regularly monitor risk events and to report errors / risk incidents as soon as they occur.

Monitoring and review are important part of the Risk Management process. Without proper monitoring and review, the Risk Management process will lose its effectiveness and may become irrelevant. Monitoring and review is an ongoing process and is essential for keeping the Risk Management process valuable and ensures that all the important information through different stages of the Risk Management process is recorded, used, and maintained.

The monitoring and review step is applicable throughout the Risk Management process (establish context, risk assessment and risk treatment). It is necessary to monitor risks, the effectiveness of the selected risk strategies and the Risk Management process as a whole.

Considerations during risk monitoring and review process

Key Factors	Description
Establish context	Initially when Risk assessment context is established, it was based on a number of factors including operational environment, stakeholder expectations, regulatory requirements, political and economic situation at that time. The monitoring and review process should be able to detect if any of these assumptions have changed, or if new factors have emerged that impact upon the context of the specific risk assessment.
Risk assessment and Controls effectiveness	The selected assessment technique and its result needs to be monitored to ensure that reliable information for risk consequences and likelihood are obtained. The control status also needs to be monitored and reviewed to make sure that controls are as effective as assessed initially or have become weak or lost effectiveness. This will ensure timely detection of these changes so that appropriate action can be taken.
Treatment strategy	This area of monitoring and review ensures that the selected treatment strategy is effectively achieving the desired objective of mitigating the risk. It helps to make sure that selected strategies are in-line with organization objective and if not, required changes are made.

The Risk register is used to monitor and review the controls and the effectiveness of action plans. For the review of the Risk Management process, there are three levels defined.

Levels of Risk Review

Review Category	Scope	Details
Regular review	• Covers day-to-day activities • Activities involved in routine work	• Provide assurance that existing controls are effective and are within the acceptable tolerance levels • Risk register can be used as a tool to record the effectiveness of current control
Functional review	• Exercise initiated by functional management on top of regular review • Executed through defined control self-risk assessment and key risk indicators (KRI)	• Activity initiated by the functional management to ensure required controls and risk treatment is effective.
External review	• Internal / external audit review with pre- defined scope of either selective areas of Risk Management process or the whole process.	• Provides third party independent perspective. • Main focus is effectiveness of selected treatment strategies. • Results in highlighting areas of improvement to enhance Risk Management practices.

To ensure adequate management support, regular reporting on the status of enterprise and operational risks is mandatory. Formal reporting is considered the main communication tool to keep the management apprised of the state of risks.

The risk monitoring activities should be prioritized based on the following:

- Enterprise risks (strategic and Extreme/High risks).
- Failure of treatment strategy would result in high consequences; and
- Residual risk ranking.

4.6 Risk Communication and Awareness

Risk communication is applicable throughout the Risk Management process. Risk communication involves the exchange of information about the nature of risk and Risk Management process. Risk communication can be inside organizations, departments or divisions, entities or outside to external stakeholders. An ineffective risk communication would lead to a breakdown in trust between the stakeholders and overall poor Risk Management. Risk communication involves a two-way dialogue between stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision maker to other stakeholders.

Effective risk communication is important to ensure that those responsible for implementing Risk Management, and those with interest in organizations successful operations, are aware of the decisions being made and provides the reason why those actions are required to ensure that organization achieves its objectives.

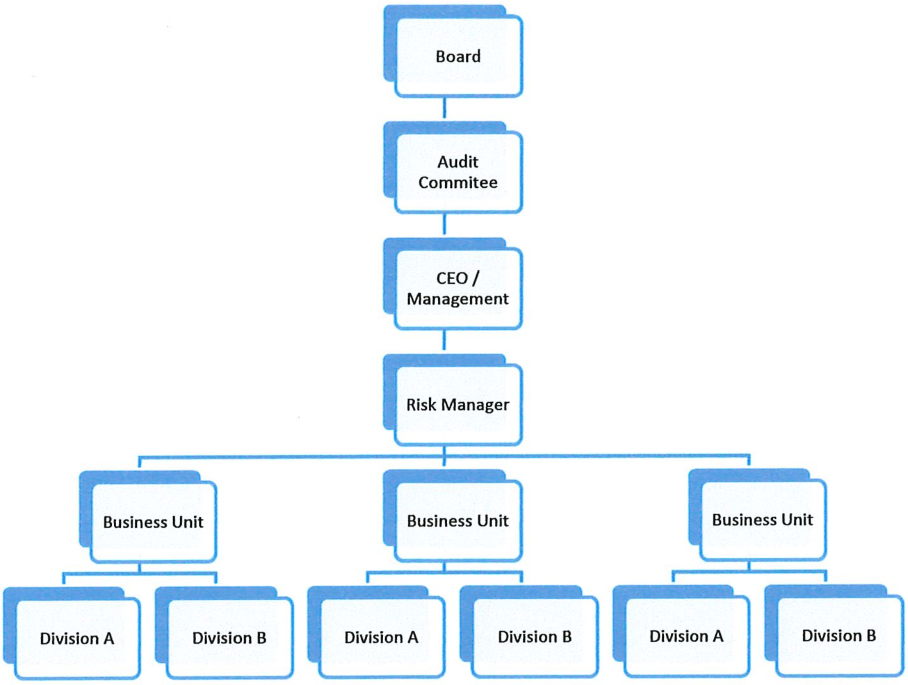
Communication and awareness is structured around the objective it is set to achieve. Some of the common objectives of this step involve:

- Identifying the stakeholders for a particular risk assessment.
- Risk assessment techniques to be applied.
- Building awareness and understanding about a particular risk or issue.
- Learning from stakeholders.
- Influencing the target audience by increasing their awareness level.
- Develop a better understanding of the Risk Management process; and
- To develop a risk aware culture.

4.7 Risk Reporting & Escalation

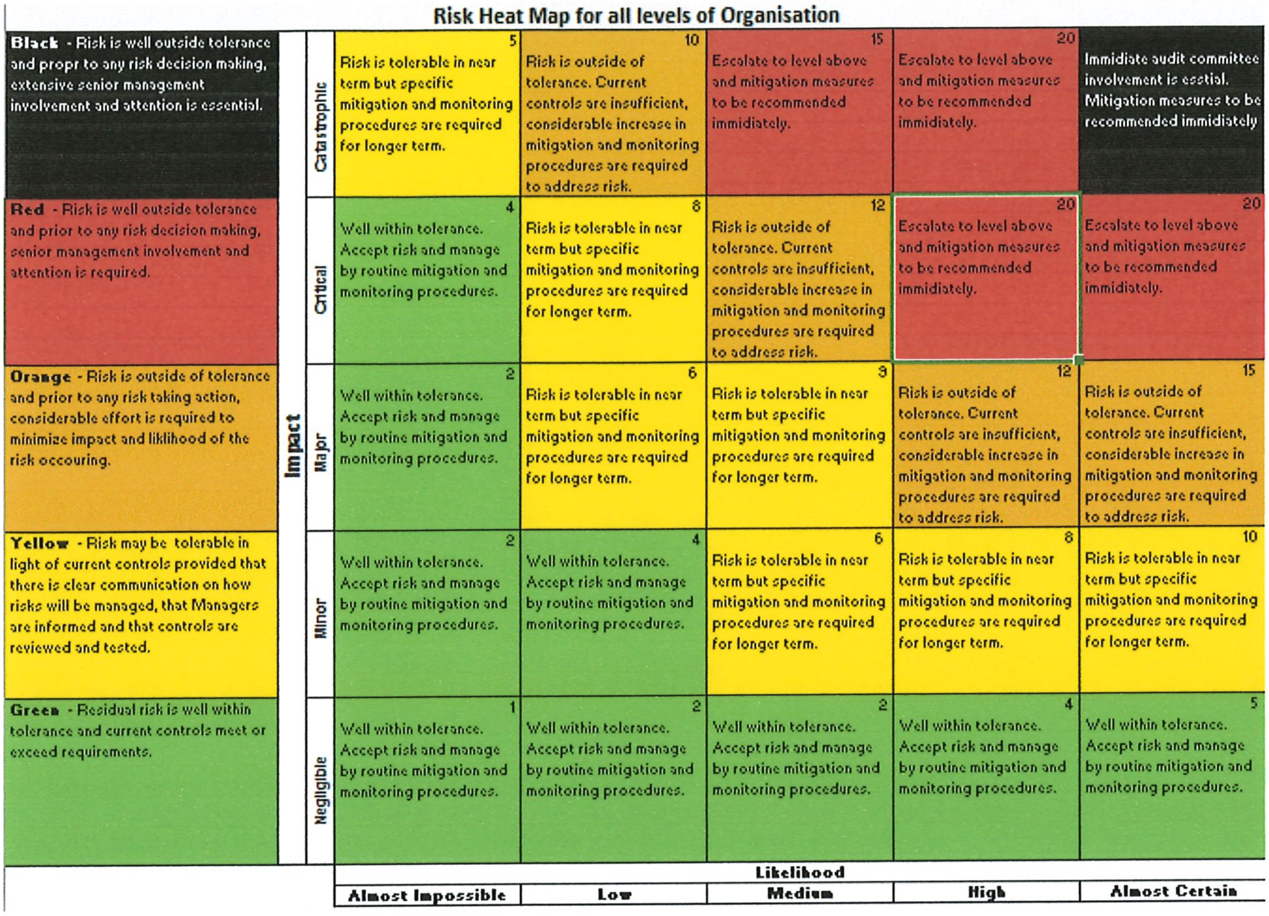
Depending on the stakeholders, the information reports are prepared to fulfil management requirements at each level.

Risk reporting shall follow the reporting structure as per Tier ownership/ risk management structure. Reports (See Appendix B) will be provided to each level.



Detailed qualitative and quantitative reporting is conducted and made available for Executive Management and Board review (if required). Key issues are highlighted and dashboards are drawn out of the risk assessment results.

The escalation of risk process is demonstrated below:

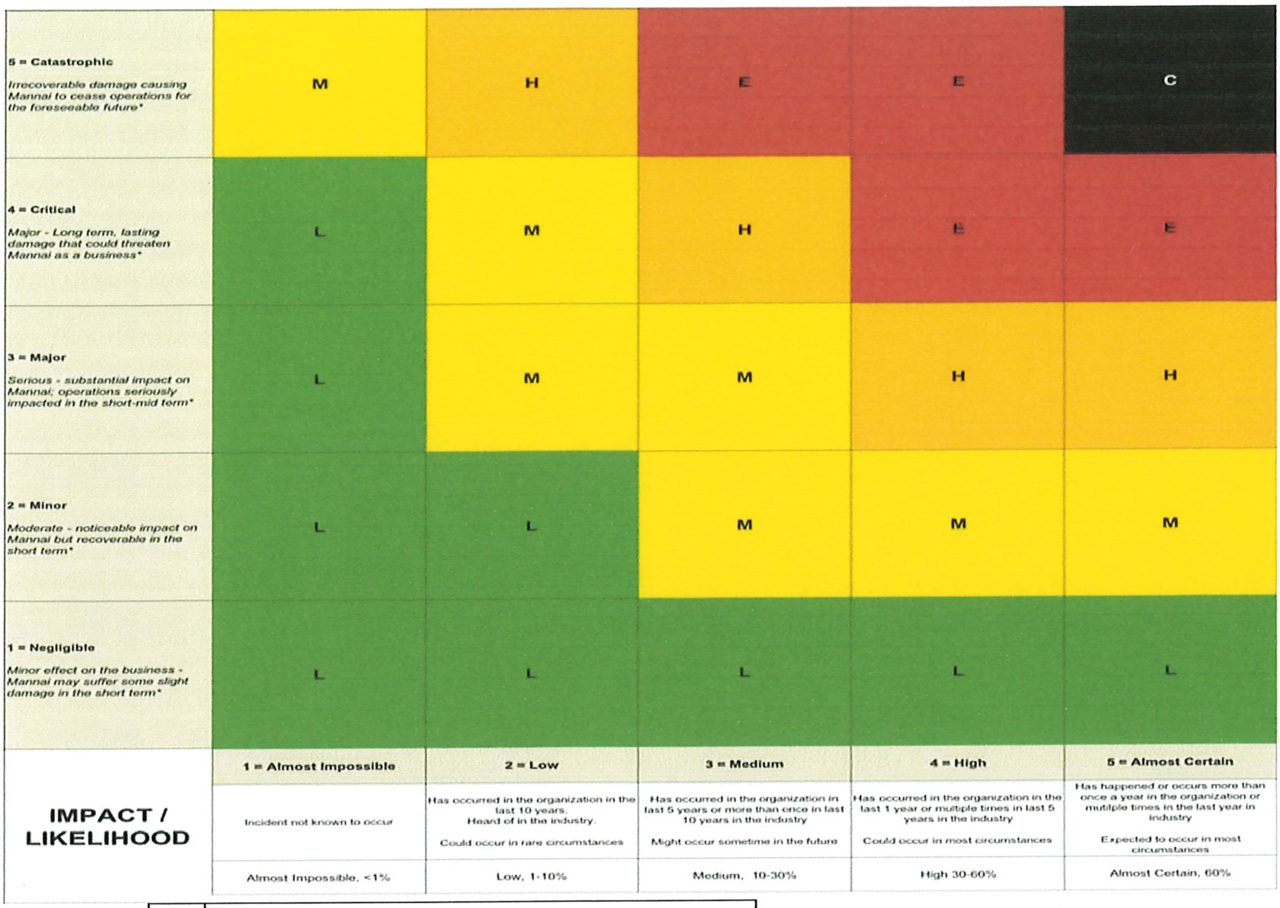


Risk Heat Map for all levels of Organisation

Black - Risk is well outside tolerance and propr to any risk decision making, extensive senior management involvement and attention is essential.	Impact	Catastrophic	5 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	10 Risk is outside of tolerance. Current controls are insufficient, considerable increase in mitigation and monitoring procedures are required to address risk.	15 Escalate to level above and mitigation measures to be recommended immidiately.	20 Escalate to level above and mitigation measures to be recommended immidiately.	Immidiate audit committee involvement is esstial. Mitigation measures to be recommended immidiately
Red - Risk is well outside tolerance and prior to any risk decision making, senior management involvement and attention is required.		Critical	4 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	8 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	12 Risk is outside of tolerance. Current controls are insufficient, considerable increase in mitigation and monitoring procedures are required to address risk.	20 Escalate to level above and mitigation measures to be recommended immidiately.	20 Escalate to level above and mitigation measures to be recommended immidiately.
Orange - Risk is outside of tolerance and prior to any risk taking action, considerable effort is required to minimize impact and liklihood of the risk occouring.		Major	2 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	6 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	9 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	12 Risk is outside of tolerance. Current controls are insufficient, considerable increase in mitigation and monitoring procedures are required to address risk.	15 Risk is outside of tolerance. Current controls are insufficient, considerable increase in mitigation and monitoring procedures are required to address risk.
Yellow - Risk may be tolerable in light of current controls provided that there is clear communication on how risks will be managed, that Managers are informed and that controls are reviewed and tested.		Minor	2 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	4 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	6 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	8 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.	10 Risk is tolerable in near term but specific mitigation and monitoring procedures are required for longer term.
Green - Residual risk is well within tolerance and current controls meet or exceed requirements.		Negligible	1 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	2 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	2 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	4 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.	5 Well within tolerance. Accept risk and manage by routine mitigation and monitoring procedures.
			Likelihood				
			Almost Impossible	Low	Medium	High	Almost Certain

5 Tools and Techniques

The risk matrix is the key tool used in the analysis and evaluation of risk. It is one of the central elements of the ERM framework and its use and application is described in the section below. Typically, the risk matrix is developed early in the lifecycle of ERM, but is reviewed regularly, usually in response to the organizations risk tolerance or appetite change.



5 = Catastrophic *Irrecoverable damage causing Mannai to cease operations for the foreseeable future**	M	H	E	E	C
4 = Critical *Major - Long term, lasting damage that could threaten Mannai as a business**	L	M	H	E	E
3 = Major *Serious - substantial impact on Mannai; operations seriously impacted in the short-mid term**	L	M	M	H	H
2 = Minor *Moderate - noticeable impact on Mannai but recoverable in the short term**	L	L	M	M	M
1 = Negligible *Minor effect on the business - Mannai may suffer some slight damage in the short term**	L	L	L	L	L
IMPACT / LIKELIHOOD	**1 = Almost Impossible**	**2 = Low**	**3 = Medium**	**4 = High**	**5 = Almost Certain**
	Incident not known to occur	Has occurred in the organization in the last 10 years. Heard of in the industry. Could occur in rare circumstances	Has occurred in the organization in last 5 years or more than once in last 10 years in the industry Might occur sometime in the future	Has occurred in the organization in the last 1 year or multiple times in last 5 years in the industry Could occur in most circumstances	Has happened or occurs more than once a year in the organization or mutliple times in the last year in industry Expected to occur in most circumstances
	Almost Impossible, <1%	Low, 1-10%	Medium, 10-30%	High 30-60%	Almost Certain, 60%

#	Description
C	Catastrophic
E	Extreme
M	Medium
L	Low

On a periodic basis (every 2 years) the risk matrix thresholds/intervals should be reviewed. Adjustments may be made in response to changes in objectives, strategy, plans business environment or other factor.

6 Roles and Responsibilities

6.1 The Board

- The Board's responsibilities for oversight of management of risk and internal controls are set out in its Charter which includes:
  - Setting, reviewing and directing risk management policies and procedures.
  - Setting the rules and procedures for implementation of control systems appropriate for risk management by generally forecasting the risks that the Company may encounter and disclosing them transparently.
  - Developing awareness programs necessary for spreading the culture of self-control and risk management of the Company.
- Approve risk appetite statements.
- Responsible for approving the final Corporate Risk Register

6.2 Audit Committee

- As per the QFMA Code, the Audit Committee shall Submit a proposal to be adopted by the Board that shall include the Company's plan in risk management that at least includes identifying major risks that may impact the Company especially those related to new technology, the Company's ability to take risks, put in risks identification mechanisms to ensure its qualification and implement awareness programs and ways to mitigate them.
- Responsible for finalising the Corporate Risk Register for Board approval. Review the Risks escalated by Risk Working Groups and provide support to manage them.
- Below is the extract of the Terms of Reference of the Audit Committee in respect of Risk Management:
  - Reviewing the systems of risk management.
  - Preparing and submitting periodic reports about risks and their management in the Company to the Board - at a time determined by the Board - including its recommendations, and preparing reports of certain risks at the behest of the Board or the Chairman.
  - Developing and reviewing regularly the Company's policies on risk management, taking into account the Company's business, market changes, investment trends and expansion plans of the Company.
  - Supervising the training programs on risk management prepared by the Company, and their nominations

6.3 Management

- Ensuring implementation of the risk management system, policies & procedures approved by the Board of Directors.
- Responsible for implementation of risk improvement recommendations.
- Allocate resources necessary to manage risks within their area of responsibility.
- Optimize business processes or decision making based on the outputs of risk management processes. Identify, assess and treat risks associated with business activities or decision-making within their area of responsibility.
- Implement the risk appetite statements.
- Accountable for ensuring the risk is managed appropriately.
- Embed risk management into all aspects of normal business processes.
- Ensure risk management identification workshops are performed on a regular interval to ensure risk register are current.

6.4 Risk Manager

- Will facilitate the introduction and maintenance of a 'holistic' risk management approach into key areas and a risk aware culture.
- Coordinate risk management activities and provide methodological support for decision making, planning, budgeting and performance management.
- Provide risk management training and integrate principles of risk management into training programs.

- Implement activities designed to integrate risk management principles into the overall organizational culture.
- Periodically review current risk procedures and identify areas for improvement.
- Responsible for reviewing Business Unit risks/registers and considering whether they should be escalated to the Strategic Risk register and communicated to the Audit Committee.
- Submit periodical report on risk management to the Audit Committee and Board and the status of key risks.
- Develop, maintain and update Risk Management policies and procedures.
- Review legal and regulatory requirements that may significantly impact on risk including any related compliance documents.
- On a periodic basis the risk matrix thresholds/intervals should be reviewed by Risk Manager and approved by Audit Committee.

6.5 Risk Working Group

- Comprises of Business Unit Heads and Risk Manager.
- Review Top risks from the Business Units for consideration for escalation to the Corporate Risk Register.
- Review Top risk actions and movement.
- Review Key Risk Indicators.
- Discuss Risks across Business Units to ensure all risks are actively managed cross functionally.
- Ensures appropriate analyses are made to define the likelihood and potential exposure.
- Responsible for Business Unit risks/registers and escalation of top risks to the Risk Manager.

6.6 Risk Owners

- Responsible for identifying, communicating and managing risks in their area of operations.
- Preparing risk analysis documentation on risks related to their area of operations.
- Report incidents which demonstrated a lack of effective risk management.
- Identify action plans, action owners, and due dates and regularly update management and risk registers accordingly.
- Implement controls and recommend additional action that results in improvement of existing or development of new controls.

6.7 Risk Champions

The RC's are responsible for the day to day co-ordination and management of all risk activities within their area of responsibility. They are also responsible for liaising with the Risk Manager and Division /Business Unit Heads on the risk communication and risk management process. Their accountabilities include:

- To engineer an environment where risk management is promoted, facilitated and appropriately undertaken within their function, and to provide the framework, tools and techniques that ensure consistency of approach.
- To bring any irregularities, gaps or concerns to the attention of the Risk Manager & Division /Business Unit Heads.

- Provide appropriate briefings / reports to the Risk Manager and Division / Business Unit Heads on a regular basis and review the current risk procedures and identify areas for potential improvement in their function.
- Monitor progress on action plans developed as part of the risk management process.

6.8 All individuals & Divisions

- Everybody working for the Company should be aware and accountable for the identification and management of risks within their area of operations.
- Responsible for reporting risks to their line managers.

6.9 Internal Audit

- Develop a risk based internal audit programme to assess the effectiveness of internal controls.
- Periodically submit to the Audit Committee a report on the Internal Control achievements.

  From Risk Management perspective the report should include:
  - Procedures of control and supervision in respect of risk management.
  - Review of the development of risk factors in the Company and the appropriateness and effectiveness of the systems in the Company.
  - The Company's compliance with Internal Control systems when determining and managing risks.
  - The risks faced the Company, their types, causes and the actions taken in this regard.
  - The suggestions for addressing the violations and mitigating the risks.

6.10 External Auditor

The External Auditor shall inform the Board in writing about any risk to which the Company is exposed or expected to be exposed, and about all of the violations immediately upon identification, as well as send a copy of that notice to the QFMA.

7 Review and Approval

This procedure document will be reviewed on an annual basis.

8 Appendices

Appendix A: Risk Register
Appendix B: Risk Report
Appendix C: Risk Management Training Plan

Approvals

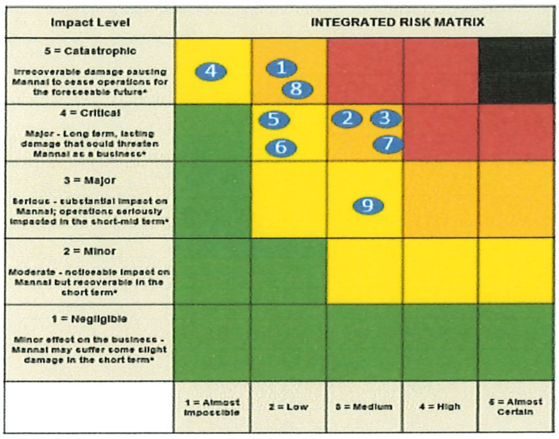
Alekh Grewal Group CEO & Director	
Ewan Cameron Group CFO	
Sheikh Khalifa Bin Abdulla Al Thani Chairman – Audit Committee	
Sheikh Suhaim Bin Abdulla Al Thani On behalf of Board of Directors	

Appendix A: Risk Register

No.	Ref	Division	Internal/ External /Both	Category of Risk	Causes	Risk	Consequences	Risk Owner	Likelihood	Impact	Final rating	Proposed Actions	Action Owner	Key Dates

Appendix B: Risk Reports (Templates)

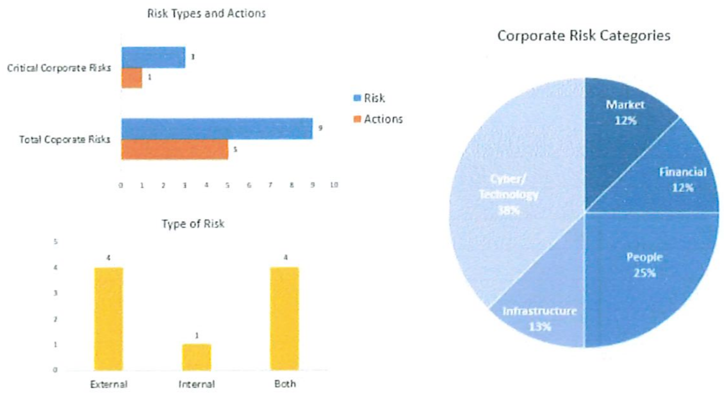
Risk Number	Top Corporate Risks	Trend



Impact Level	INTEGRATED RISK MATRIX				
5 = Catastrophic Irrecoverable damage causing Mannal to cease operations for the foreseeable future*	🟨 4	🟧 1 8	🟥	🟥	⬛
4 = Critical Major - Long term, lasting damage that could threaten Mannal as a business*	🟩	🟨 5 6	🟧 2 3 7	🟥	🟥
3 = Major Serious - substantial impact on Mannal; operations seriously impacted in the short-mid term*	🟩	🟨	🟨 9	🟧	🟧
2 = Minor Moderate - noticeable impact on Mannal but recoverable in the short term*	🟩	🟩	🟨	🟨	🟨
1 = Negligible Minor effect on the business - Mannal may suffer some slight damage in the short term*	🟩	🟩	🟩	🟩	🟩
	1 = Almost Impossible	2 = Low	3 = Medium	4 = High	5 = Almost Certain

Number of total Risks in Organization	
Number of total actions	
Number of Total Critical Risks	
Number of total actions for critical risks	

Corporate Risks



Appendix C: Risk Management Training Plan

ENTERPRISE RISK MANAGEMENT TRAINING PLAN

1.1 Purpose
The purpose of the training plan is to identify the appropriate training strategies and activities required to achieve the desired learning outcome for the all the employees to support the functioning of effective Enterprise Risk Management (ERM).

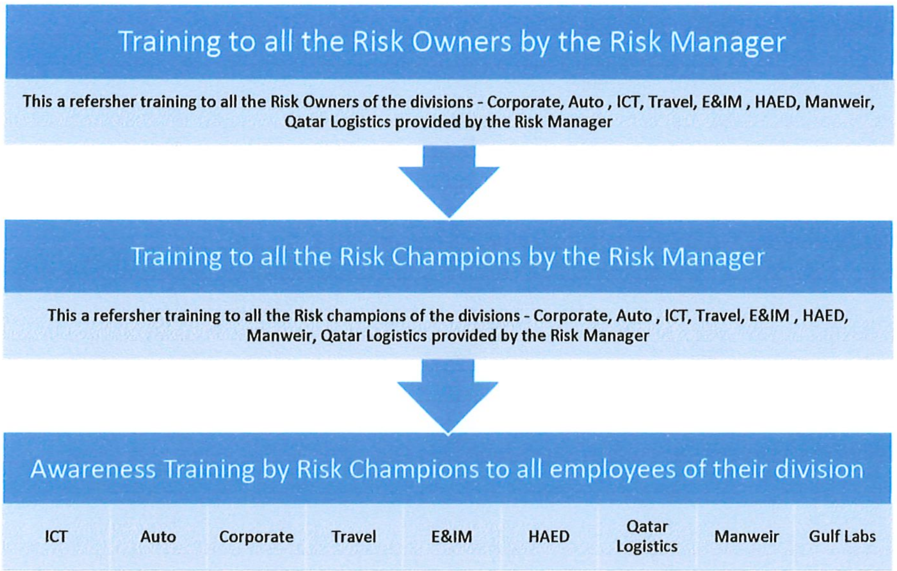
1.3 Training Objectives
The training is designed to focus on key principles and concepts of risk management and aimed at setting the context both internal and externally, identifying and assessing risk to objectives as well as looking at approaches to managing risk. Additionally, the training looks at how risk communication plays a vital part in the success of risk management.
The program is designed to raise awareness in an interactive manner to ensure that attendees are equipped with the right skill set and knowledge.

The objectives for the Training Plan are:

- *Identifying the stakeholders for a particular risk assessment.*

- *Risk assessment techniques to be applied.*
- *Building awareness and understanding about a particular risk or issue.*
- *Learning from stakeholders.*
- *Influencing the target audience by increasing their awareness level.*
- *Develop a better understanding of the Risk Management process; and*
- *To develop a risk aware culture.*

2. TRAINING METHOLODOGY



Training to all the Risk Owners by the Risk Manager

This a refersher training to all the Risk Owners of the divisions - Corporate, Auto , ICT, Travel, E&IM , HAED, Manweir, Qatar Logistics provided by the Risk Manager

Training to all the Risk Champions by the Risk Manager

This a refersher training to all the Risk champions of the divisions - Corporate, Auto , ICT, Travel, E&IM , HAED, Manweir, Qatar Logistics provided by the Risk Manager

Awareness Training by Risk Champions to all employees of their division

ICT

Auto

Corporate

Travel

E&IM

HAED

Qatar Logistics

Manweir

Gulf Labs

Measuring Effectiveness & Feedback

The effectiveness of training is measured throughout its duration through multiple techniques, including assessments, and obtaining feedback and regular check points.