E.A. TECHNIQUE (M) BERHAD
ENTERPRISE RISK MANAGEMENT (ERM) POLICY

ERM Policy Statement of E.A. Technique (M) Berhad ("EATech")

EATech recognises that it is obliged to systematically manage and regularly review its risk profile at a strategic, financial, operational and compliance level. EATech proposes to do this by developing / adopting risk management framework that determines the process and identifies tools for realising its objectives. Not only does it wish to minimise its risk but also maximise its opportunities. It enhances EATech's capability to respond timely to the changing environment and its ability to make better decisions.

The Risk Management Framework's scope is Group-wide. The application of the policy will be the responsibility of Chief Operating Officer ("COO") with content input from those with accountability in specific areas. Head of Departments/ Managers at all levels are accountable for risk management.

Risk Registers are developed and subject to regular review at Risk Management Committee ("RMC") level and subsequently ranked, debated, and reported to the MD, Management Committee ("MC"), Board Audit Committee ("AC"), and Board of Directors ("the Board").

The Board has a stewardship responsibility to understand these risks, provide guidance on dealing with these risks and to ensure risks are managed proactively, in a structured and consistent manner.

The objectives of the policy statement are to ensure:

- a common and consistent approach for management of risks is adopted within EATech Group;
- the management of risk contributes to the quality of performance and continuous improvement of EATech businesses, its operations and delivery of services and products; and
- all significant risks are identified, evaluated, managed and reported on a timely manner to the RMC, MC, AC and the Board.

The policies of the Board for Enterprise Risk Management ("ERM") are:

- To integrate risk management into the culture, business activities and decision-making processes. Risk management concept, thinking and initiatives must be embedded in a day-to-day business operation and decision making process. Risks that can be managed through embedded, routine systems and processes should be so managed and monitored. Where risks cannot be so managed, they must be subjected to individualised risk management techniques appropriate to a particular risk.

- To anticipate and respond to the changing operational, social, environmental and regulatory requirements proactively.
  As far as reasonably possible, risks must be identified, analysed and dealt with by management proactively based on their experience, industry knowledge and information available from the market place. EATech must not experience any crystalisation of major risk unexpected by the Board. However, this does not mean the risk will not happen, but there are comprehensive plans put in place to respond timely and address the risk impact.

- To manage risks pragmatically, to an acceptable level given the particular circumstances of each situation.
  In dealing with risks, the Board understands that it is not always possible, cost effective or desirable to manage or eliminate risk all together. A cost-benefit approach is needed where the returns must commensurate with the risks taken and reduce cost of risk controls.

- To implement a robust and sustainable ERM framework that is aligned with EATech's vision and missions, and in accordance with best practices.
  The Board recognises that a structured and consistent ERM framework is instrumental for EATech to deploy its operational strategy effectively.

These policies will be achieved via: -

- Periodic reporting to the Board on risk management activities and keep the Board apprised and advised of all aspects of ERM and significant individual risks and risk trends;
- Provision of adequate and suitable resources, including tool(s) and manpower to ensure the ERM framework and system are operating effectively;
- Provision of adequate education and communication to ensure staff comprehend the requirements, benefits, and their role and responsibilities for risk management; and
- Maintaining documented risk information (via risk registers and risk action plans) and procedures for the control of risks.

Periodic Review:

This ERM Policy will be periodically reviewed to ensure the needs of the Company are met as well as to encompass any development in framework, rules and regulations that may have an impact on the EATech's ERM processes or practices.

ENTERPRISE RISK MANAGEMENT (ERM) FRAMEWORK

CONTENTS PAGE

Introduction

The International Organisation for Standardisation - ISO 31000:2010 defines risk management as the "coordinated activities to direct and control an organisation with regard to risk".

This International Standard recommends that organisations develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. Risk management can be applied to an entire organisation, at its many areas and levels, at any time, as well as to specific functions, projects and activities.

This policy confirms EATech's commitment to adopting a strategic, consistent and structured enterprise-wide approach to risk management in order to achieve an appropriate balance between realising opportunities for gains and minimising losses. The policy reflects the ISO 31000:2010 which provides the overall framework for risk management at EATech.

Risk management is an integral part of sound management practice and an essential element of good corporate governance; involves establishing an appropriate risk management infrastructure and culture, and applying logical and systematic risk management processes to all stages in the life cycle of any activity, function or operation.

The function of risk management is to provide a sound contribution to the achievement of EATech's corporate objectives and to support the strategic directions of the Group through the systematically manage and regularly review its risk profile at a strategic, financial, operational and compliance level. It enhances the understanding of the potential upside and downside of the factors that can affect an organisation.

Definitions

EATech will adopt a consistent terminology in relation to risk to ensure effective communication and stakeholder awareness of risk and risk management within the Group **(*Please See Glossary at Page 19*).**

Governance and Management

Specific roles and responsibilities for risk management in EATech are as follows:

Role	Principal responsibilities for ERM
Board of Directors	▪ Adopt the ERM Policy; ▪ Articulate and provide direction on risk appetite, organisational control environment and risk culture at EATech; ▪ Final decision on risk parameters, risk appetite, risk profiles, risk treatment options, and risk action plans; ▪ Assess and keep abreast with key risk indicators; and ▪ Monitor the overall ERM framework's performance and implementation effectiveness at EATech.
Audit Committee (AC)	▪ Provide an objective view on the effectiveness of ERM and internal controls as a whole to the Board, reviews and approves internal and external audit plans and monitors risk reporting; ▪ Act as an advisor, educator and change catalyst in risks and control areas in the organisation; ▪ Provide an independent view on specific risk and control issues, the state of internal controls, trends and events; and ▪ Actively requests and challenges risk information from the business.
Risk Management Committee ("RMC")	▪ Assist the Board in establishing and maintaining effective policies and guidelines to ensure proper management of risks to which Group is exposed and to take appropriate and timely action to manage such risks; ▪ Review and endorse the risk parameters, risk appetite, risk profiles, risk treatment options, risk action plans and key risk indicators; ▪ Communicate requirements of the ERM Policy to staff and ensure continuous enhancement of ERM; ▪ Formulate and implement ERM mechanism to accomplish requirements of the ERM policy; ▪ Discuss, rank and debate risk ratings, control effectiveness, risk treatment and action plans identified by RO; and ▪ Ensure that the ERM reports prepared are submitted to Board of Directors in a timely manner, and special risk report / flash reports are submitted in the event of any risk(s) that required urgent attention.
Risk Management Coordinator ("RMC")	▪ Continuously communicate, evaluate and improve the ERM Policy and ERM mechanism; ▪ Facilitate the risk assessment, implementation of risk action plan and key risk indicators process; ▪ Prepare risk parameters, risk appetite, monitoring of risk action plans and provide independent review on key risk indicators; ▪ Provide independent input on risk assessment (risk types and risk ratings), and action plans comprehensiveness; ▪ Conduct risk identification, evaluation and review of risk treatment process on a periodic basis to ensure the Group's risk management effectiveness; ▪ Prepare and report to the RMC in a timely manner, and ensure special risk report / flash report is prepared in the event of any risk(s) that required urgent attention; and ▪ Lead the ERM educational programmes, and continuous sharing insights into risk and market trends with RO.

Risk Owners (RO)	▪ Identification and assessment of risks, implementation and monitoring of risk action plans and key risk indicators; ▪ Prepare and report to RMC on a timely manner and timely preparation of flash reports in the event of any risk(s) that required urgent attention; and ▪ Maintain highest alert on both internal and external activities or circumstances that may have adverse risk impacts and consequences to EATech.
Risk Co-owners	▪ Provide support to RO on key risks identified and to assist in the implementation of risk action plans and key risk indicators thereof; and ▪ Engage and discuss with RO on internal and external activities or circumstances that may give rise to new risks or changes on rating or control effectiveness of existing risks.
Staff	▪ Provide assistance to RO and / or Risk Co-owners on key risks identified and to support the implementation of risk action plans and key risk indicators; and ▪ Engage and discuss with RO and / or Risk Co-owners on internal and external activities or circumstances that may give rise to new risks or changes on rating or control effectiveness of existing risks.
Internal Audit Department	▪ To assist Audit Committee in reviewing the effectiveness of ERM and internal controls and providing an independent view on specific risks and control issues, the state of internal controls, trends and events.

***Figure1**: Specific roles and responsibilities for risk management.*

While Management team members are accountable for risk management in their particular portfolios, responsibility for good risk management rests with every staff member. This includes execution of jobs in a professional, careful and conscientious manner that contributes to the high ethics and culture within the Group.

Enterprise Risk Management Approach

Risks will be managed according to EATech's Enterprise Risk Management Framework which is based on the ISO 31000:2010 - Risk Management Process.

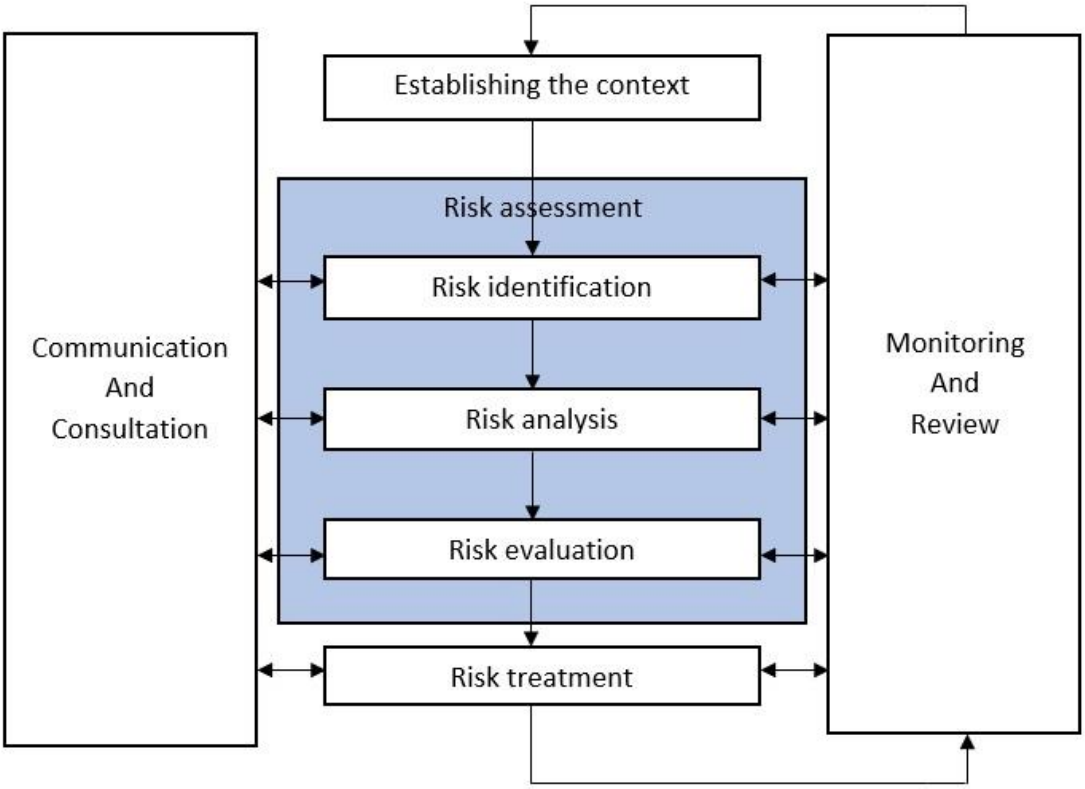


Figure 2: *The ISO 31000:2010 - Risk Management Process*

1) **Communication and Consultation**

EATech considers both external and internal factors as well as within or beyond the Group control when communicating and consulting associated with the achievement of strategic and operational objectives. Communication and consultation with external and internal stakeholders should take place during all stages of the risk management process.

Plans for communication and consultation should be developed at an early stage. These should address issues relating to the risk, its causes, its consequences and the measures being taken to treat it.

2) **Establishing the Context**

The organization articulates its objectives, defines the external and internal parameters to be considered when managing risk, and sets the scope and risk criteria for the remaining process.

2.1) **Establishing the External Context**

The external context can include, but is not limited to:

- The social and cultural, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- Key drivers and trends having impact on the objectives of the organization; and
- Relationship with, perceptions and values of external stakeholders.

2.2) **Establishing the Internal Context**

Internal context is anything within the organization that can influence the way in which an organization will manage risk

2.3) **Establishing the Context of the Risk Management Process**

The objectives, strategies, scope and parameters of the activities of the organization where the risk management process is being applied, should be established. The resources required, responsibilities and authorities, and the records to be kept should also be specified.

2.4) **Defining risk criteria**

The criteria should reflect the organization's values, objectives and resources. Risk criteria should be consistent with the organization's risk management policy.

When defining risk criteria, factors to be considered should include the following:

- The nature and types of causes and consequences that can occur and how they will be measured;
- How likelihood will be defined;
- The timeframe(s) of the likelihood and/or consequence(s);
- How the level of risk is to be determined;
- The view of stakeholders;
- The level at which risk becomes acceptable or tolerable; and
- Whether combinations of multiple risks should be taken into account and if so, how and which combinations should be considered.

3) **Risk assessment**

The overall process of risk identification, risk analysis and risk evaluation. This is one of the key elements in ERM methodology.

3.1) **Risk Identification**

Risk identification is a process when an organization should identify sources of risk, areas of impacts, events and their causes and potential consequences.

The aim of this step is to generate a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives.

Comprehensive identification is critical, because a risk that is not identified at this stage will not be included in further analysis.

3.2 **Risk analysis**

Risk analysis involves developing an understanding of the risk. The risk analysis should be started with determine the root causes / sources of risk, assess the ***likelihood*** and ***impact*** to produce a Gross Risk Rating.

Likelihood and impact can be determined by modelling the outcomes of an event or set of events, or from experimental studies or from available data. Impact can be expressed in terms of financial and non-financial impacts.

3.3 **Risk evaluation**

The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation.

Decisions should be made in accordance with legal, regulatory and other requirements.

EATech has identified relevant ***likelihood*** and ***impact ratings***, as shown in the ***Figures 4, 5 and 6;*** and then translated into ***Overall Risk Rating Matrix*** as per ***Figure 7***.

In addition to assessing likelihood and impact ratings, the **Effectiveness of Existing Controls** should also be considered in terms of the ***Rating Level*** as illustrated in ***Figures 8*** *and* **9**.

Description	Risk Description
Almost Certain	Probability of **81% - 100%** of event happening; or More than **6 events** a year
Likely	Probability of **61% - 80%** of event happening; or **1 – 5 events** in a year
Possible	Probability of **31% - 60%** of event happening; or **Once (1) a year**
Unlikely	Probability of **11% - 30%** of event happening; or **Once (1) in 5 years**
Remote	Probability of **10% or less** of event happening; or **Once (1) in 10 years**

Figure 4: *Likelihood Rating*

Financial		IMPACT				
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
TIER 1 EATech	Profit Before Tax	Reduce By **<5%**	Reduce By **5%-10%**	Reduce By **10%-20%**	Reduce By **20%-30%**	Reduce By **> 30%**
TIER 2 JSE	Profit Before Tax	Reduce By **<5%**	Reduce By **5%-10%**	Reduce By **10%-20%**	Reduce By **20%-30%**	Reduce By **> 30%**

Figure 5: *Impact Rating – Financial (The impact rating is compare against the approved budget)*

Non financial	IMPACT				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Legal/Regulatory / Compliance	No litigation consequences	Issuance of reprimand/ warning latter	Issuance of public reprimand/ warning letter	Multiple issuance of reprimands / warning letters	Loss of license / certification
	Issuance of advice letter	Minimum fine	Moderate fine	Heavy fines	Closure of operations
				Suspension of share	Jail sentence for directors
Reputations / Media	Minimum impact	Minor impact due to complaints	Significant media coverage	Serious media coverage/ negative public image	Adverse local / international media coverage with authority intervention that could cause the organisation's reputation to sustain long-term/ permanent damage/ disruption to business
	No permanent damaged in the short-or-long term	Unfavorable media coverage that would not disrupt the organisation routine operations	Public's complaints to authority/ stakeholders/ press that could disrupt the organisation's operations in the short-or-medium-term	Authority takes actions against the organisation that could disrupt the organisation's business in certain period of time	
Safety	Injuries with no treatment or repair on asset at no cost	Injuries with first aid treatment or minor repair on the asset with minor cost	Medical treatment required or damage on asset has to be repaired with high cost	Extensive injuries that effect productivity or major repair required on the asset with very high cost	Death or huge repair with huge cost required
General Statement	An event where the impact can be absorbed/ managed through routine activity	An event where the impact can be absorbed/ managed with minimum management effort	An event that cause the business to sustain negative financial / non – financial impact that would require some work/ planning from management to manage the issue	An event that could lead the business to sustain huge adverse financial/ non-financial impact that would require hard work from management to manage the issue	An event that could potentially crumple the entire business in the long-term

Figure 6: *Impact Rating – Non-Financial*

		Impact				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Almost Certain	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	High
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Medium	Medium	High

Figure 7: *Overall Risk Rating Matrix*

Level	Action
Extreme	Must be managed by top management with detail action plan
High	Senior management input or attention is required
Medium	Managed by routine procedures or the risk may be worth accepting with monitoring
Low	Unlikely to need specific application of resources or may accept the risk

Figure 8: *Risk Level Rating*

Description	Control Description
Satisfactory	Controls are well managed, operated properly, and meet compliance requirements.
Some weaknesses	Some control weaknesses / inefficiencies have been identified. Although they do not present serious risk exposures but improvements in the controls are required.
Weak	Unsatisfactory controls and do not meet acceptable standards, as many control weaknesses / inefficiencies have been identified.

Figure 9: *Effectiveness of Existing Controls*

4) **Risk treatment**

Risk treatment involves selecting one or more options for modifying risks and implementing those options. Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived.

Once a treatment has been implemented, it becomes a control or it modifies existing controls. Risk treatment involves a cyclical process of:

– Assessing a risk treatment;
– Deciding whether residual risk levels are tolerable;
– If not tolerable, generating a new risk treatment; and
– Assessing the effectiveness of that treatment.

EATech has five main ways in which it can effectively **manage/treat risks**, as follows:

1. **Accept** - accept the risk and make a conscious decision to not take any action.
2. **Taking** - in order to pursue an opportunity.
3. **Reduce** - accept the risk but take some actions to lessen or minimise its likelihood or impact.
4. **Transfer** - transfer the risk, for example outsourcing / contract the activity; or by financing (insure against) the risk; or joint ventures.
5. **Avoid** - eliminate the risk by ceasing to perform the activity that gives rise to the risk.

Risk Action Plan (RAP)

In many organisations, one of the most challenging parts in ERM implementation is developing, implementing and monitoring the risk action planning.
The purpose of risk action plans is to document how the chosen treatment options will be implemented.

EATech has established its risk action plans implementation practices through the following process:

- Identifying the Risk Owner and Co-Owner;
- Update root causes and existing controls;
- Identify risk treatment options and it rationale;
- Prepare detail risk action plans, time frame and person-in-charge; and
- Estimate expected implementation cost.

The information provided in treatment plans should include:

- the reasons for selection of treatment options;
- those who are accountable for approving the plan and those responsible for implementing the plan;
- proposed actions;
- resource requirements including contingencies;
- performance measures and constraints;
- reporting and monitoring requirements; and
- timing and schedule.

Treatment plans should be integrated with the management processes of the organisation and discussed with appropriate stakeholders.

In ensuring the agreed risk action plan being appropriately implemented, EATech recognised that the Follow Up process is important to be carried out on periodically basis.

The action plan should also clearly identify the priority order in which individual risk treatments should be implemented.

4.1) **Selection of risk treatment options**

When selecting risk treatment options, the organization should consider the values and perceptions of stakeholders and the most appropriate ways to communicate with them. Where risk treatment options can impact on risk elsewhere in the organization or with stakeholders, these should be involved in the decision.

The treatment plan should clearly identify the priority order in which individual risk treatments should be implemented.

Risk treatment itself can introduce risks. A significant risk can be the failure or ineffectiveness of the risk treatment measures. Monitoring needs to be an integral part or the risk treatment plan to give assurance that the measures remain effective.

Risk treatment can also introduce secondary risks that need to be assessed, treated, monitored and reviewed. These secondary risks should be incorporated into the same treatment plan as the original risk and not treated as a new risk. The link between the two risks should be identified and maintained.

4.2) **Preparing and implementing risk treatment plans**

The purpose of risk treatment plans is to document how the chosen treatment options will be implemented. The information provided in treatment plans should include:

- the reasons for selection of treatment options, including expected benefits to be gained
- those who are accountable for approving the plan and those responsible for implementing the plan
- proposed actions
- resource requirements including contingencies
- performance measures and constraints
- reporting and monitoring requirements
- timing and schedule

The residual risk should be documented and subjected to monitoring, review and where appropriate, further treatment.

5) **Monitoring and review**

EATech's environment is constantly changing and hence needs to continually monitor and review its risks and the effectiveness of its management of risk over time.

The period of risk review will be determined by the risk rating, with higher rated risks and associated controls/risk mitigation strategies reviewed more often.

Monitoring and review can be periodic or ad hoc, should be a planned part of the risk management process and involve regular checking and surveillance.

Risk monitoring and review will:

- ensure risks appropriately reflect the reality of the EATech's operating environment;
- involve the review of risk ratings (likelihood & Impact);
- involve a review of the adequacy and effectiveness of existing risk controls / treatment plans and recommend changes to treatment priorities & timeframes;
- identify emerging or new risks; and
- include consideration of the appropriate "responsible person(s)" for ongoing monitoring and review of risks.

Additionally, monitoring and measuring includes evaluation of the risk awareness culture and the risk management framework, and assessment of the extent to which risk management tasks are aligned, suitable, adequate, and effective way of achieving established objectives.

This will enable the internal audit function to periodically review the effectiveness of risk management function in EATech and providing an independent view on specific risks and control issues, the state of internal controls, trends and events.

In general, ISO 31000 expects EATech to review the risk management framework and risk management process. It specifically expects for EATech to review the risk management policy and plans as well as risks, risk categories, risk treatments, controls, residual risks, and risk assessment process.

Based on results of monitoring and reviews, decisions should be made on how the risk management program can be improved. These decisions should lead to improvements in the organisation's management of risk and its risk management culture.

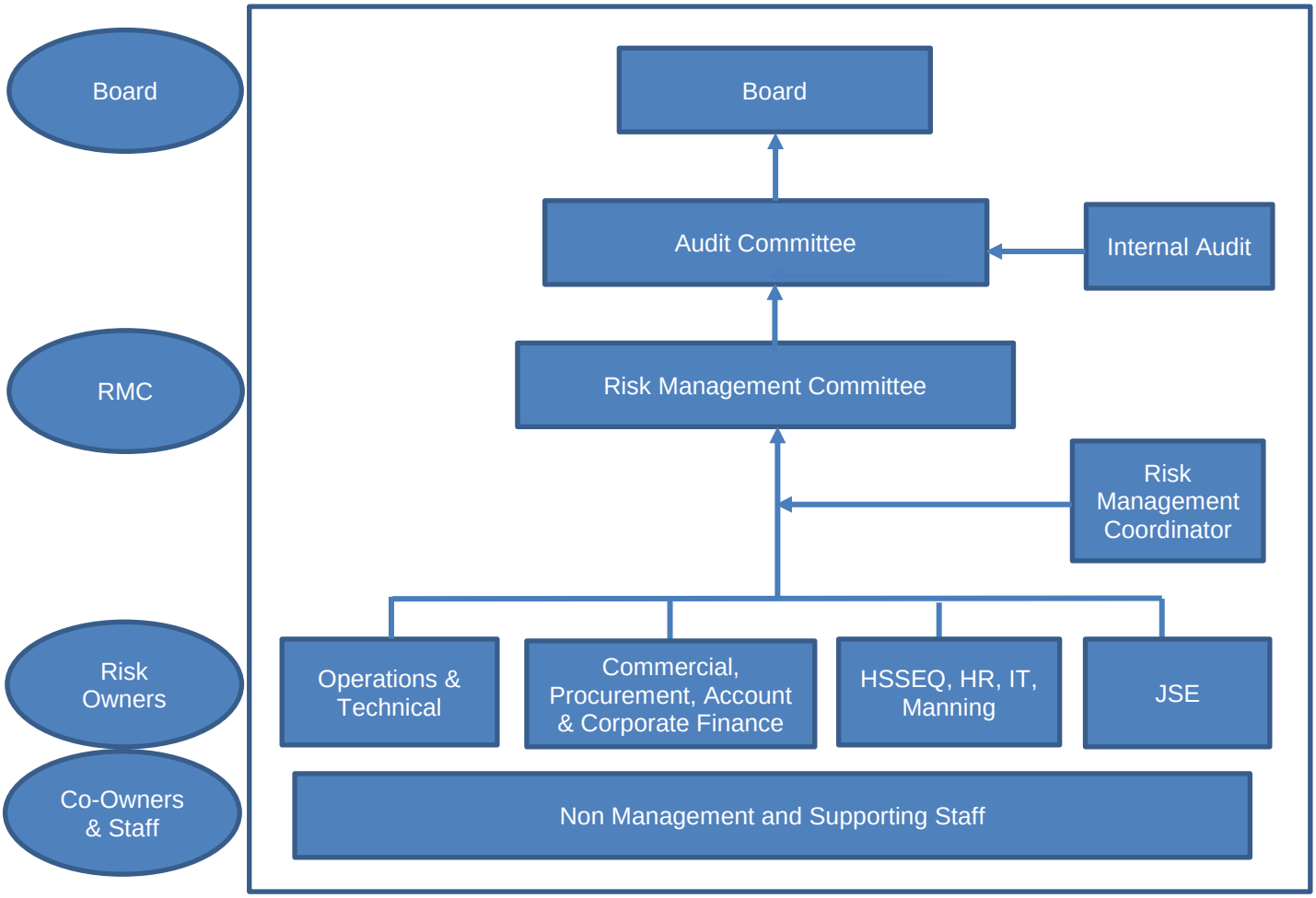


Figure 10: *EATech's ERM Risk Reporting Structure*

Reporting party	Reporting to	Frequency of reporting	Reports to be submitted
Risk Management Coordinator	Board of Directors	Quarterly	• Group risk profile • Risk action plans and status updates for top 10 risks (of the Group) • Special risk report/flash report on need basis
	Audit Committee	Quarterly	• Full and/or Special risk report / flash report on need basis
	Risk Management Committee	Quarterly	• Updated business unit risk profiles and risk registers • Risk action plans and status updates • Special risk report / flash report on need basis
Risk Owners	Risk Management Coordinator	Quarterly	• Updated operations risk profiles and risk registers • Risk action plans and status updates • Special risk report / flash report on need basis
Co-Owners	Risk Owners	Monthly	• risk profiles and risk registers • Risk action plans and status updates • Special risk report / flash report on need basis
Internal Audit	Audit Committee	Annually	• Independent report on the effectiveness of the risk management and internal control activities as a whole

Figure 11: *EATech's ERM Risk Reporting Frequency*

6) **Recording the risk management process**

EATech's environment is constantly changing and hence needs to continually monitor and review its risks. Risk management activities should be traceable. In the risk management process, records provide the foundation for improvement in methods and tools, as well as in the overall process.

Enterprise Risk Management Program

Principles

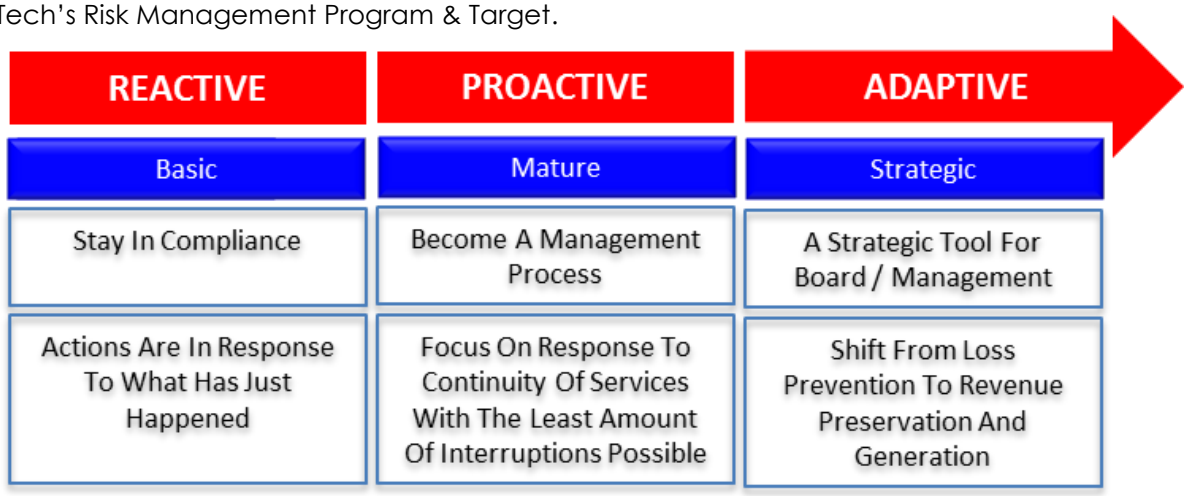
EATech's **vision** for future risk management is to have a culture in which risk is managed in an integrated manner that will enable the Company to:

- be recognised as a leader with best practice management; to achieve the Company's Vision, Mission and Business Goals
- achieve financial and operational goals (both in financial budgets, and as detailed in the annual budget)
- be the high ethics' organisation that managing its risks responsibly.

Education

Creating a risk awareness culture in the Company is a crucial part of implementing and sustaining a robust risk management and compliance programme. In addition to providing training and support for those with portfolio responsibilities in the areas of risk and compliance, opportunities will also be provided for all staff to engage in regular training opportunities about relevant risk and compliance issues. Further, the CRO will develop and disseminate tool kits that raise awareness about risk management and statutory compliance obligation.

EATech's Risk Management Program & Target.



Appendix A: Sample of Risk Register

Risk Register

Department	**HSSEQ**
Specific risk	**Exposure to acts of piracy**
Description	Merchant ships or vessels run the risk of being targeted by pirates during a voyage, especially for ships that carry large quantities of high-value goods including CPP. Refer attached list of acts of piracy.

Root causes:	**Existing key controls:**
1. Our Company operates within piracy prone areas.	1. We have adopted the necessary anti-piracy measures including installation of the press alert button. Further, GPS (SHIPLOC) is installed to track down the vessels in the event of pirate attack. 2. We have shipping insurance policies to ensure that we are compensated for some of the losses incurred in the event of piracy attack. 3. We have Rotation Duty Manager every weekly for Safety and Security Monitoring. 4. Red area is highlighted to All Vessel that trading in the high risk area (Tawau, Singapore Straits). 5. Operation to Alert Vessel and HSSE dept (to inform APMM) whenever vessel transiting Red Area for monitoring.

	Likelihood	**Impact**	**Risk rating**
Gross risk	Possible	Moderate	High
Residual rating	Possible	Insignificant	Low

Glossary

ISO 31000:2010, Risk management – Principles and guidelines

The Risk Management standard to which EATech's risk management policy aims to adhere to.

ISO 31000:2010 provides principles, framework and a process for managing risk. It can be used by any organisation regardless of its size, activity or sector. However, ISO 31000 cannot be used for certification purposes, but does provide guidance for internal or external audit programmes. This Standard was published on November 2009. ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management.

ISO 31000:2010 has been received as a replacement to the existing standard on risk management.

Assurance
A process that provides confidence that planned objectives will be achieved within an acceptable degree of risk.

Consequence / Impact
The outcome of an event affecting objectives.

Control
Any action taken to manage risk. These actions may be taken to manage either the impact of the risk if realised, or the likelihood of the risk.

Event
Occurrence or change or a set of circumstances.

Enterprise Risk Management (ERM)
Is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

Gross Risk
The initial assessment of a risk without any controls in place.

Likelihood
Chance of something happening.

Residual Risk
Risk that remain after all existing controls have been implemented.

Risk
Effect of uncertainty on objectives.

Risk Appetite
The amount of risk that EATech is prepared to accept or be exposed to at any point in time.

Risk Owner (RO)
A person or entity that has been given the authority to manage a particular risk and is accountable for doing so.

Risk Co-Owner (RCO)
Person or entity which provides support to RO on key risks identified and to assist in the implementation of risk action plans.

Risk Management
Coordinated activities to direct and control an organisation with regard to risk.

Risk Management Framework
A set of components that support and sustain risk management throughout an organization.

Risk Management Policy
A policy statement defines a general commitment, direction, or intention. A risk management policy statement expresses an organization's commitment to risk management and clarifies its general direction or intention.

Risk Management Process
Systematic application of the steps: establishing the context, identifying, analysing, evaluating, treating, communicating, consulting monitoring and reviewing risk.

Risk Profile
A risk profile is a written description of a set of risks. A risk profile can include the risks that the entire organisation must manage or only those that a particular function or part of the organization must address.

Risk Rating
The rating resulting from the application of the risk assessment matrix on the likelihood and impact of a risk occurring.

Risk Register
A system or file that holds all information on identifying and managing a risk. It specifies: a description of the risk, its root causes and its impacts; an outline of the existing controls; an assessment of the consequences of the risk should it occur and the likelihood of the consequence occurring, given the controls; a risk rating; and an overall priority for the risk.