ACAP ADVISORY PUBLIC COMPANY LIMITED

RISK MANAGEMENT FRAMEWORK

ACAP ADVISORY PUBLIC COMPANY LIMITED

February, 2010

ACAP ADVISORY PCL

Risk Management Framework

Table of Contents

Appendix

Risk Management Framework

1. Objectives

To implement a systematic program across the organization to effectively manage risks involved in the Company's pursuit of its businesses of non-performing asset management, investment banking advisory, consumer finance, and related businesses, and to assure shareholders, stakeholders, directors, management and other personnel that the risks involved in the performance of the Company's business activities are understood and efficiently managed to achieve the following:

1. **Strategic Focus:** Decision-making aimed at minimizing risks and maximizing the Company's current and future growth and profitability.
2. **Operational Efficiency:** Effective and efficient use of the Company's human resources, material resources and financial resources.
3. **Full Compliance:** Ensure all staff complies with applicable laws and regulations of the Company and that the Company complies with all applicable governmental laws and regulatory authorities' rules and regulations.
4. **Financial Reporting:** Ensure the soundness and integrity of the Company's financial statements and financial reports that are used for both internal and external reporting purposes.

2. Risk Management Policy Statement

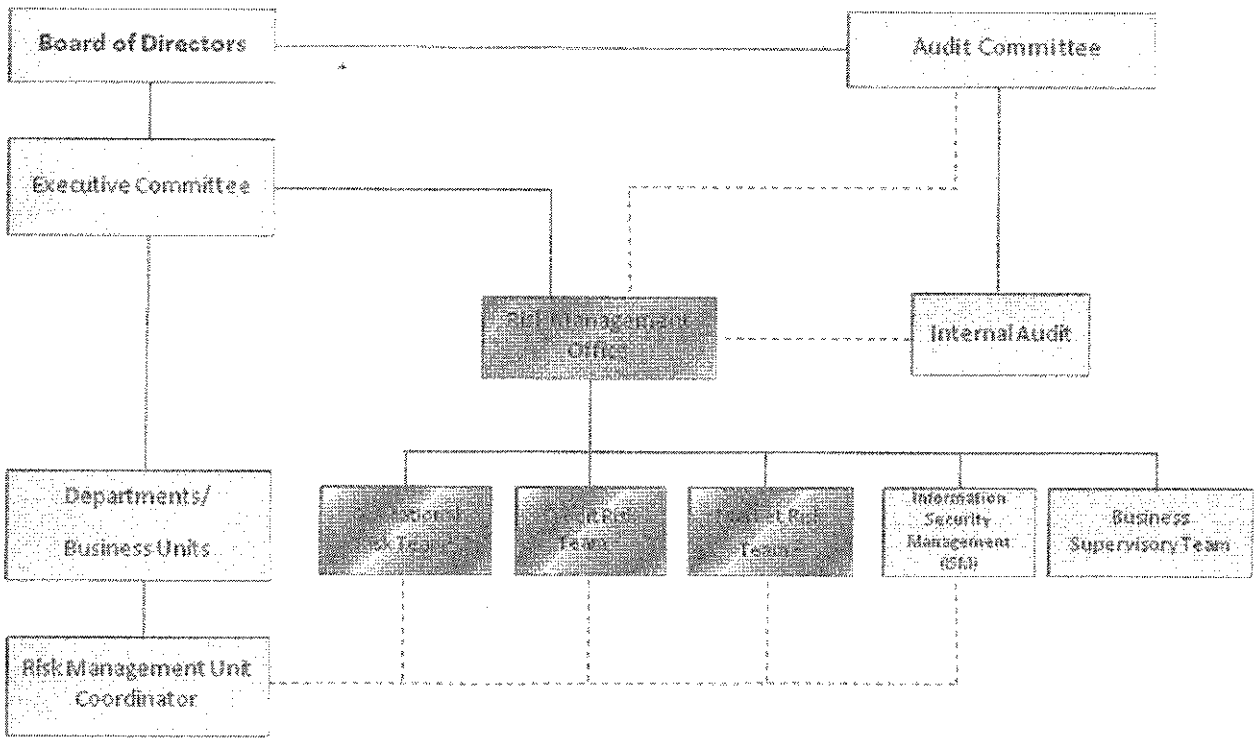
The Company's policy is to establish effective risk management processes and routines throughout the organization and to encourage all managers and employees at all levels to participate in risk management activities as part of the Company's corporate culture. The Risk Management Framework is to be included as part of the *Company's Operations Procedures Manual* and work policy for each department, which will require each department and their staffs to execute risk management practices and activities according to their assigned roles and responsibilities.

3. Definitions of Risk and Risk Management

Risk is defined as any event that can impact on the Company's realization or achievement of its strategic, operational, and/or financial objectives.

Risk Management is the set of systematic processes and activities aimed identifying, assessing, mitigating/treating and monitoring the factors that cause risk and uncertainty in the Company's achievement of its strategic, operational, and/or financial objectives. This also includes development of the policies, procedures and plans governing these processes and activities, whose objective is to prevent or minimize adverse effects on the Company's business operations.

4. Risk Management Structure



*Notes: [1] Key Business Unit Managers shall participate as part of Operational Risk Team.

[2] Operational Risk Team is in process. Credit Risk & Market Risk Teams will be set up once these risks are deemed to be significant.

5. Roles and Responsibilities of Parties

5.1 Board of Directors

- Advise and approve the Company's *Risk Management Framework*.

5.2 Executive Committee

- Approve the processes and procedures for implementing the Company's risk management policy and *Risk Management Framework*.
- Appoint the *Risk Management Office* to supervise implementation of the risk management processes and procedures under the *Risk Management Framework* that should cover all risks applicable to the Company's on-going businesses, including *operational risk, credit risk, market risk, information security risk, business risk, strategic risk,* etc., and should be appropriate for the Company's operations.
- Assign Department/Business managers and other personnel to participate as members of the various Risk Management Teams as required.
- Approve risk threshold levels for each type of risk as proposed by RMO.
- Approve business unit risk management plans and the Company's *Risk Management Procedures Manual.*
- Encourage all managers and staffs at all levels to participate in risk management activities as part of the Company's corporate culture.

5.3 Audit Committee

- Monitor the Company's overall risk management processes and procedures.
- Report on the effectiveness of the Company's risk management processes/plans and internal control process to the Board of Directors and shareholders.
- Work with the *Risk Management Office* to ensure mutual understanding of risks and to ensure that the risk management processes and internal control process are consistent.

5.4 Risk Management Office (RMO)

- Supervise implementation of risk management plans, and the *Risk Management Framework* and *Risk Management Procedures Manual,* which should cover all risks applicable to the Company's on-going businesses, including *operational risk, credit risk, market risk, information security risk, business risk, strategic risk,* etc., and should be appropriate for the Company's operations.
- Appoint *Risk Management Teams,* as appropriate, to pursue the risk management plans for the given type of risk (i.e. *operational risk, credit risk, market risk, etc.*).
- Propose to the Executive Committee the appropriateness of risk threshold levels (i.e. maximum tolerable risk) for each type of risk that have been determined with RMTs.

- Monitor the Company's strategic risk for consistency with its risk tolerance and risk management policies, and report on strategic risk to the Audit Committee.
- Submit and present the *Risk Management Summary Report,* covering risk assessment, risk control, risk management and risk mitigation, to Audit Committee each quarter.
- Prepare the *Risk Management Overview Report* each year and present to Audit Committee for approval and announcement in the Company's Annual Report.
- Review the Company's risk management policy, processes and mitigation plans annually and present *Risk Management Continuity Report* to the Audit Committee every year.

5.5 Risk Management Teams (RMTs)

- Apply the *Risk Management Framework* to the particular risk for which they are responsible.
- Identify, analyze and assess actual and potential risks (internal and external), their probabilities of occurrence and their impacts on corporate performance, as well as determine appropriate risk thresholds (i.e. maximum tolerable risk).
- Develop and prepare *Risk Management Plans*, including detailed risk mitigation plans with specific actions, responsible parties and timeframes.
- Support and advise the business units on their execution of risk management processes.
- Act as a center of risk management control process, and work closely with and monitor Risk Management Unit Coordinators.
- Evaluate results of actions in *Risk Management Reports* monthly or quarterly and submit to Internal Audit.
- Prepare the *Risk Management Summary Report* covering risk assessment, risk control, risk management and mitigation, and evaluate the progress of risk management and mitigation plans each quarter and report to RMO.
- Review and revise the risk management plans for improvement and effectiveness every year and report to RMO. This information is the basis for the *Risk Management Continuity Report.*
- Perform other related functions as assigned by RMO.

5.6 Information Security Management Department

- Manage *information security risk* throughout the Company covering five key areas, including physical environment, hardware and software, applications, networks and people and reports results regularly (i.e. quarterly) to RMO and Audit Committee.
- Attain key security mechanisms of Confidentiality, Availability, and Integrity in addition to Accountability and Access Control.

- Achieve best practices for Information security defined by trusted sources (ISO17799/ISO27001, ITIL, CoBiT, BOT security requirements, etc.) to support the business requirements and directions of the Company.

5.7 Business Supervisory Team

- Supervise compliance by all Parties at the Company with all Agreements entered into with Portfolio Investors and Stakeholders (i.e. Shareholders, Creditors, etc.) to control *business risk*.
- Review on regular basis (i.e. quarterly) compliance with, among others, Sale & Purchase Agreements, Servicing Agreements, Loan Facility Agreements, Collection Policies and Business Plans that the Company has with Portfolio Investors and Stakeholders.
- Take follow-up actions to ensure compliance by all Parties at the Company with the above Agreements and reports results to RMO.

5.8 Departments/Business Units Managers

- Act as members of RMTs as required (i.e. specifically for *Operational Risk Team*).
- Agree to the risk management plans and be responsible for and assist their departments/business units with implementation of risk management plans.
- Encourage staff within their departments/business units to understand the importance of risk management and to engage in proper risk management practices.
- Assign their staff to follow the risk management plans.
- Appoint Risk Management Unit Coordinators.

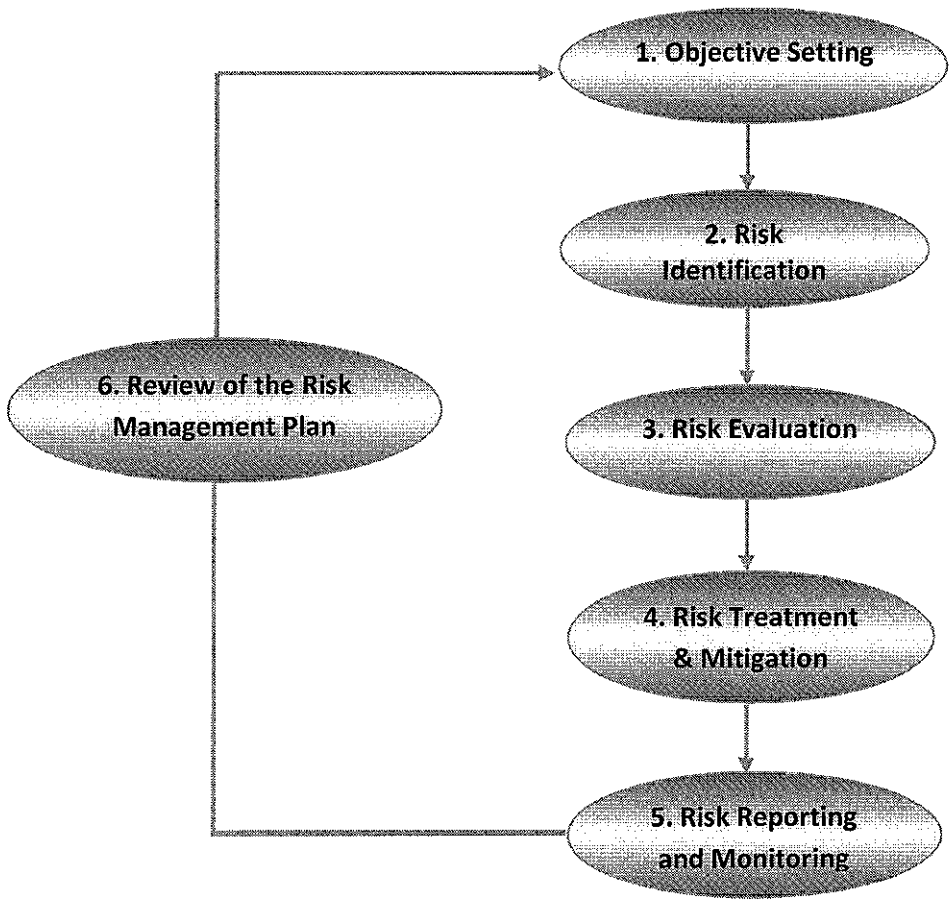
5.9 Risk Management Unit Coordinators (RMUCs)

- Facilitate and monitor progress of risk management tasks and risk management plan in their departments/business units.
- Coordinate with RMTs and report on progress of risk management tasks assigned in their business units.
- Perform other related functions assigned by RMTs and/or departments/business units.

5.10 Internal Audit Department

- Review risk management processes and procedures.
- Advise, coordinate with, and support RMO and RMTs as Internal Audit executes the internal audit process according to the risk management policy.
- Report the results of internal audits to Audit Committee.

6. Risk Management Process



Risk Management Process Consists of Six Processes

1. Objectives Setting

Objectives must be set that clearly identify the scope of work to be done and to ensure that management and staff understand the activities they must undertake to accomplish the objectives. It is important to set objectives at Business Unit or Department Levels that support and are aligned with the Company's high-level objectives. Objective setting should have the characteristics embodied by the acronym "SMART", meaning objectives should be:

- Specific
- Measurable
- Achievable
- Reasonable
- Time constrained

2. Risk Identification

The components of risk identification are as follows:

2.1 Categorize risks by type: risk can generally be categorized into the following main types, including:

- Operational Risk
- Credit Risk
- Market Risk
- Strategic Risk
- Information Security Risk
- Business Risk

Risk Management Teams and RM Plans for each Business Unit must be distinguished by type of risk involved.

2.2 Categorize by Operational Activities, including:

- Strategic
- Operations / Reporting
- Compliance
- Financial

2.3 Categorize by Organization Structure

The principles of the risk analysis process are:

- Internal and external risk events that have affected (or can potentially affect) achievement of an entity's objectives must be analyzed.
- Analysis of *Job Responsibilities* and *Work Flows* of each business unit should be done (by seminar, interview, or other sources of information) to determine actual (and potential) sources of internal risk events.

When the risk identification and analysis process has been completed, it is necessary to categorize risk and identify the obstacles and limitations to mitigating the risks that have affected the achievement of the entity's objectives.

3. Risk Evaluation

3.1 Risk Scoring: After the risk assessment is completed, the particular risk should be ranked according to its Probability of Occurrence and its Impact.

3.1.1) Assessing Probability of Occurrence (Likelihood): the likelihood that the risk would occur should be classified into one of 4 levels with the definitions as shown in the following table:

Level of Likelihood	Definition	Description
1	Low	Likely to occur occasionally
2	Moderate	Likely to occur in every year
3	High	Likely to occur in every quarter
4	Very High	Likely to occur in every day

Remark: Occasionally means less than once per year.

3.1.2) Assessing Consequences (Impact): The level of severity of potential losses, given that the risk factor occurs, should be expressed for each identified risk using a monetary range, if possible. Alternatively, the level of impact should be classified into one of 4 levels with the definitions as shown in the following table:

Level of Impact	Definitions	Descriptions
1	Low	Loss less than 0.1 million baht and impact within the unit
2	Moderate	Loss 0.1 -0.3 million baht and impact within the organization
3	High	Loss 0.3 -0.5 million baht and impact to any related party or counterparty
4	Very High	Loss greater than 0.5 million baht and impact to stakeholders and/or public

Remark: Evaluate from impact of lost revenue, including lost opportunity, and/ or increased costs.

In assessing the level of severity of the impact and the consequence of the risk, the following should be considered:

1) Financial Impact: impact or damage may be estimated with respect to:
- Affect to various departments;
- Affect to revenues, expenses or profit; and
- Others

2) Operational Impact: affect to operational procedures or servicing:
- External Impact: affect from changes in existing or new government regulations and laws;
- Affect to budgeting and reimbursement;
- Affect to operational plans; and
- Others

3) Security Impact: affect to company's properties:
- Affect to physical property (buildings, equipment, etc.)
- Affect to intellectual property (proprietary know-how);
- Affect to employees; and
- Others

4) Compliance Impact: affect to company from changes in internal and external rules and regulations:
   - Affect from changes in company's rules and regulations;
   - Affect from changes in existing or new government regulations and laws; and
   - Others

5) Customer Satisfaction Impact: affect to the level of customer satisfaction:
   - Affect to portfolio investor clients
   - Affect to individual (retail) customers/debtors
   - Affect to corporate customers/debtors
   - Affect on the Company's overall reputation

When the risk evaluation process has been completed, it is necessary to compare the estimated level of severity of impact against the possibility of risk. Risk evaluation, therefore, is used to make decisions about the significance of risks to the organization and whether each specific risk should be accepted or treated. If the company has limitations of budgeting and resources, the risks that have high severity and high possibility of occurrence should be managed and mitigated first. Treatment of risks with less severity and lower likelihood of occurring can then be handled next.

4. Risk Treatment and Risk Management Planning

4.1 Risk treatment is the process of selecting and implementing an action to modify the risk.

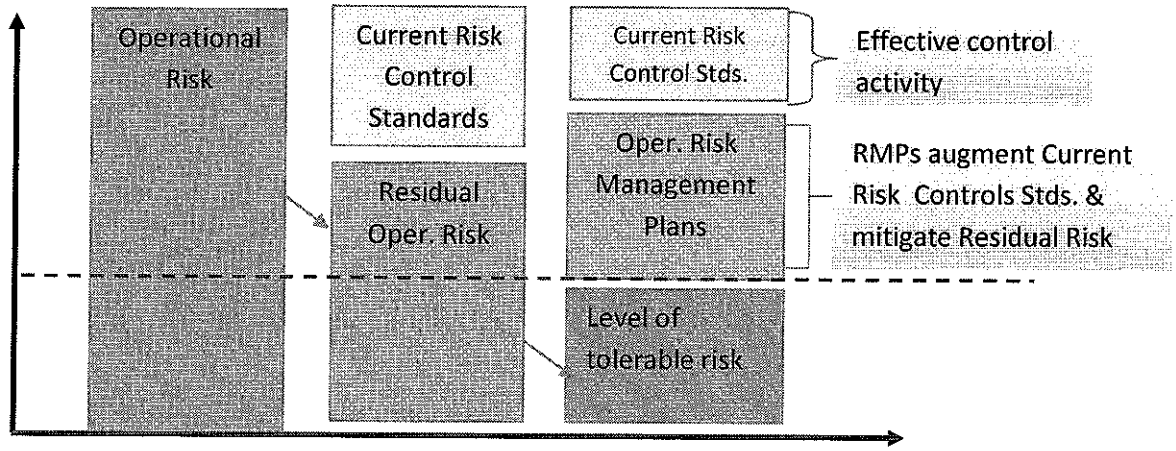
1) Risk Avoidance: aims to avoid a particular risk. For example,
   - Change the objective
   - Cease the activity

2) Risk Transfer: aims to transfer a particular risk to other party. For example,
   - Buy insurance
   - Outsource to an external agent

3) Risk Reduction / Risk Control: aims to set control activities to manage and mitigate risks. For example,
   - Develop/Implement Risk Management and Mitigation Plans
   - Modify procedures (i.e. workflows) to reduce risk
   - Set risk protection standards (i.e. maximum tolerable risk for given activities)

4) Risk Acceptance: For example,
   - Request for risk acceptance standards (i.e. conditions under which a given risk can be accepted)
   - Take no action; note this is only for risks with very low probability of occurring and very low impact

4.2 Risk Management & Mitigation Plans



Risk Management and Mitigation Plans aim to reduce risks to acceptable levels (see above diagram for example regarding Operational Risk).

4.2.1 Risk response includes developing and implementing risk control/mitigation plans. A useful way to assess risks and prioritize risk responses is by utilizing a Standard Risk Point Matrix (as described below and shown in the following diagram). This tool can be used to rank the level of risks at the Department and Business Unit levels.

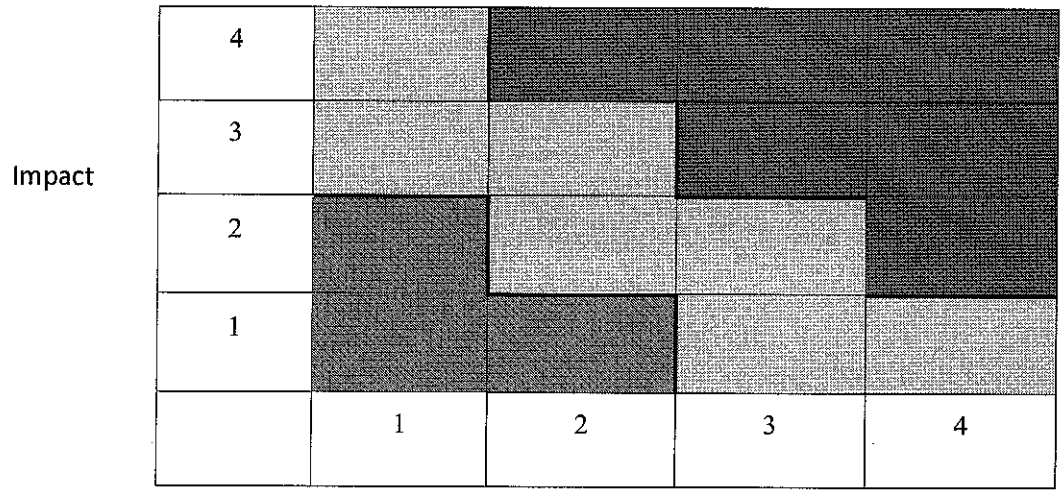
In a Standard Risk Point Matrix, the vertical axis indicates the level of Impact and the horizontal axis indicates the level of Likelihood of Occurrence. The matrix is divided into 3 risk groups: Low Level (Green Zone); Moderate Level (Yellow Zone); and High Level (Red Zone).

Red Zone: Likelihood x Impact is equal to or greater than 8. The risks in this area are a high priority and must be managed and mitigated immediately. In addition, the sources of risk, the process / procedure owners and the time frames must be clearly defined for effective and timely mitigation of these risks.

Yellow Zone: Likelihood x Impact is between 3 and 6. The risks in this area have a moderate priority, but they still must be managed and mitigated accordingly based on considerations of significance of operations or budgeting. Also, additional risk management standards may or may be not needed; however, process / procedure owners and the time frames must be clearly defined for the required risk management actions. Moreover, the risks of natural disasters (i.e. fire, flood, etc.) which have high impact but low likelihood require preparation and testing of a Disaster Recovery Plan, a part of overall Business Continuity Planning.

Green Zone: Likelihood x Impact is equal to or less than 2. The risks in this area may be generally acceptable or considered a low priority, so additional risk management actions may not be needed.

Standard Risk Matrix



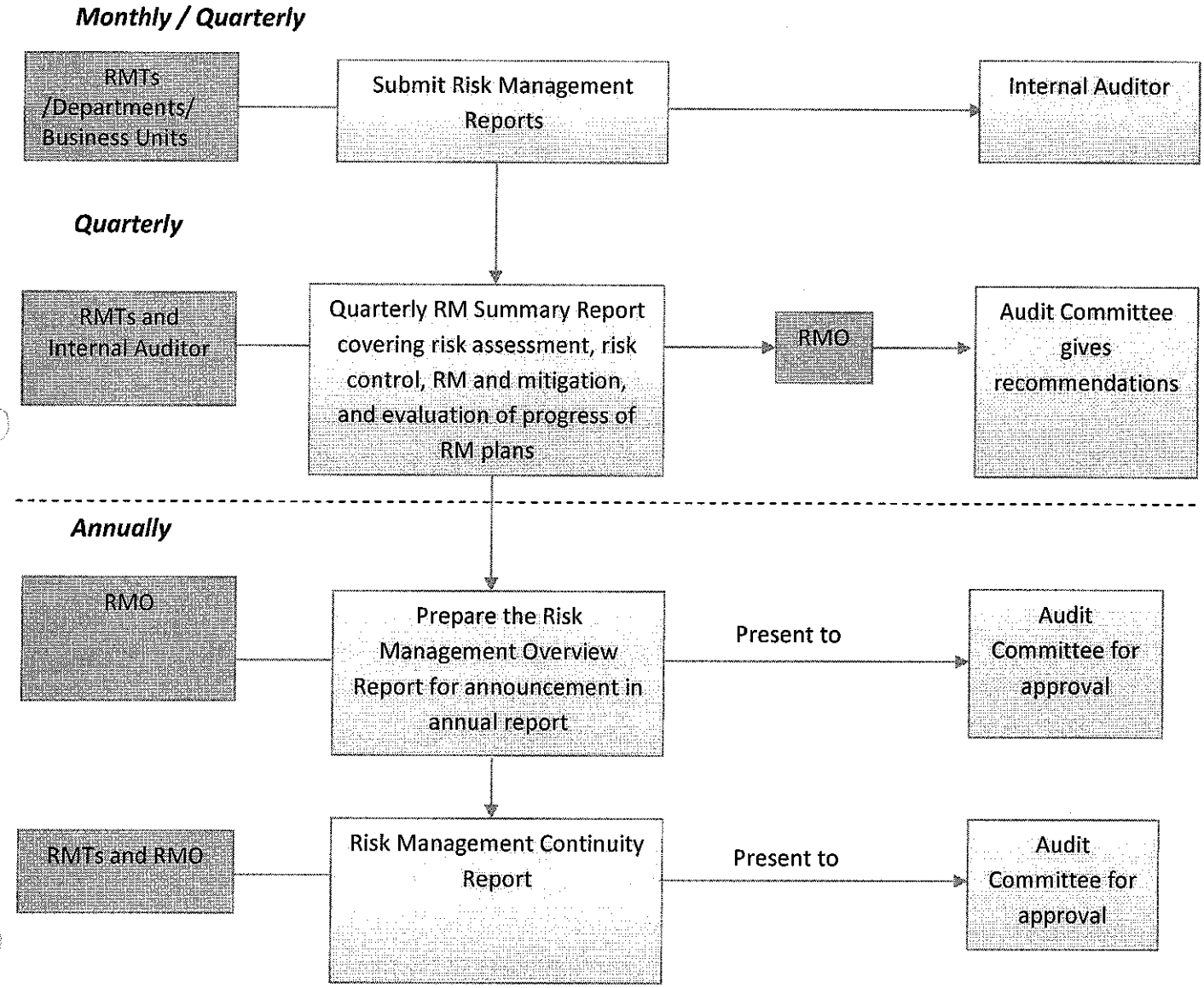
5. Risk Monitoring and Reporting

Risk Monitoring and Reporting can ensure that the Company has appropriate internal risk management, that risk control standards have been efficiently implemented within the organization, and that risk management has been appropriately implemented throughout the organization. The Risk Monitoring and Reporting process is shown in Diagram A.

6. Review of Risk Management Plans

RMTs and Internal Audit shall review, assess and summarize progress made on implementation of risk management plans in order to further assess, modify and refine these plans (where necessary) on an annual basis with Department Heads and Business Unit Managers. This information is then compiled as the Risk Management Continuity Report and presented by RMO annually to the Audit Committee for approval.

Diagram A: Monitoring, Reporting, and Review of Risk Management



Report Summary

REPORT	CONTENT	FROM	TO	FREQUENCY
1) Risk Management Procedures Manual	Details of RM Procedures, Processes, etc.	RMTs, RMO	EXCOM/ AC	On-going
2) Risk Management Reports	Evaluation of RM Activities & Actions	RMTs	IA	Monthly/ Quarterly
3) Risk Management Summary Reports	Summary of (2), including Progress on Risk Mitigation Plans	RMTs, IA, RMO	AC	Quarterly
4) Risk Management Overview Report	RM Overview for including in ACAP's Annual Report (F56-1)	RMO	AC	Annually
5) Risk Management Continuity Report	Review & Revise RM Plans, etc.	RMTs, RMO	AC	Annually

RMO: Risk Management Office
RMTs: Risk Management Teams
EXCOM: Executive Committee
AC: Audit Committee
IA: Internal Audit

Appendix

- Definitions of Types of Risk
- Forms and Tables for Risk Management

Definitions of Types of Risk

RISK TYPE	DEFINITION
Operational Risk	Operational Risk is risk from exposure to loss from inadequate or failed internal processes, people and systems, or from external events. The Bank for International Settlements has established seven (7) main categories of operational risks and these have also been adopted by the Bank of Thailand, including: • *Internal Fraud* • *External Fraud* • *Employment Practices and Workplace Safety* • *Business Practice* • *Damage to Physical Assets* • *Business Disruption and Systems Failures* • *Execution, Delivery and Process Management*
Market Risk	Market Risk is risk from exposure to the uncertain market value of a portfolio. Market risk can be in the forms of *Equity Price Risk, Foreign Currency Risk, Commodity Price Risk, and Interest Rate Risk.*
Credit Risk	Credit Risk is risk from exposure to uncertainty in a counter party's ability to meet its obligations. In addition to outright *Default*, other types of credit risk include: *Ratings Downgrades; Counterparty Failure; and Collateral Problems.*
Business Risk	Business Risk is risk from exposure to non-compliance by the Company with legal contracts and agreements entered into with 3rd parties, including Investor Clients, Lenders, Shareholders and other Stakeholders.
Strategic Risk	Strategic Risk is exposure to risks from changes in the Company's long-term strategies and related industries' trends, such as entering new businesses, operating in new countries, forming new joint ventures or engaging in M&A activities, and opportunities and threats from external trends and developments in industries covering the Company's existing and future businesses (i.e. *Regulatory Risk*), etc.
Information Security Risk	Information Security Risk is risk from exposure to unauthorized access to, use, disclosure, disruption, modification or destruction of the Company's confidential and proprietary information, including information relating to the Company's clients, customers and stakeholders, etc.

Risk Identification

Form 01

Level of Impact ❶	Dept./Unit ❷	Activities ❸	Type of Risk ❹	Potential Risk ❺	Details of Risk ❻
- Identify Degree of Risk (H, M, L)	- Line of business	Activities: 1. Strategic 2. Operational / Reporting 3. Compliance 4. Financial	There are 3 types: 1. Market Risk 2. Credit Risk 3. Operations Risk	- Identify indicators of risks or events that may affect the strategy and achievement of the business unit objectives.	- Describe the event or occurrence of risk.

Risk Assessment and Risk Scoring

Form 02

Level of Impact ❶	Dept./Unit ❷	Activities ❸	Type of Risk ❹	Potential Risk ❺	Details of Risk ❻	Likelihood of Risk Occurrence ❼	Impact of Risk Occurred ❽	Risk Score (7) x (8) ❾
Inputs - Form 01						- Map or evaluate risk with the significance and likelihood of risk occurrence (Form 03)	- Measure the impact of risk with the significance and type of risk occurred (Form 04)	- Matrix of the score of likelihood of risk ❼ and the impact of risk ❽.

Likelihood of Risk Occurrence

Form 03

Frequency of Risk/Likelihood of Risk Occurrence

Frequency of Risk / Likelihood of Risk	1 (Low) Likely to occur occasionally	2 (Moderate) Likely to occur every year	3 (High) Likely to occur every quarter	4 (Very High) Likely to occur every day

Risk Impact Evaluation

Form 04

Level of Impact

Level of Impact / Category	1 Low	2 Moderate	3 High	4 Very High
1. Financial Risk				
- Loss/Damage				
- Profit (Loss)				
2. Operational Risk				
- Risk from External Factors				
-Government's Laws and Regulations				
-Results on Business Operations				
3. Safety on Physical Assets				
- Collateral Management				
4. Compliance				
- Rules and Regulations				
5. Customer Service				
- Customer Satisfaction				

Risk Management Report

Form 05

Department/Unit_____

Month_____

Risk Factor_____

Risk Management Action Plan_____

Date of Completion _____

Responsible Person _____

Activity	Results	Estimated Time	Results from Action Performed		Problems and Suggestions
			% this month	% accumulated	

ACAP

ACAP Advisory Public Company Limited

Summary Report of Risk Assessment, Risk Control, Risk Management, and Suggestions

Form 06

Department/Unit _____

As of month _____

No.	Risk Factor	Details of Risk	Details of Risk Control	Risk Management Action Plan	Completion Date/Responsible by	Operational Results			Details of Operations		Suggestions
						Completed	Completed and On-going	On-going	Action	Results	