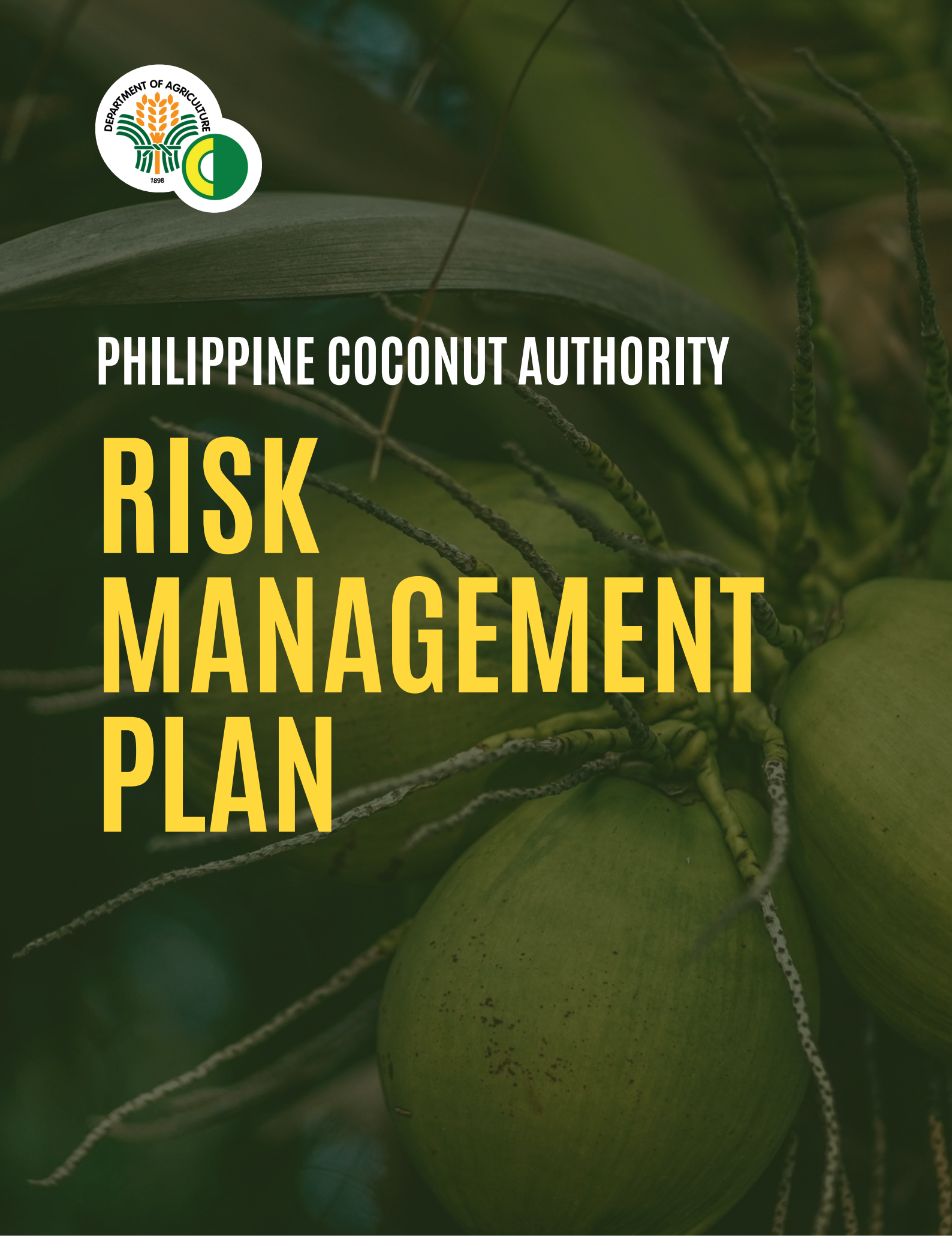


PHILIPPINE COCONUT AUTHORITY

RISK MANAGEMENT PLAN

Department of Agriculture
Philippine Coconut Authority
Elliptical Road, Diliman, Quezon City
ofad@pca.gov.ph

PHILIPPINE COCONUT AUTHORITY
RISK MANAGEMENT PLAN

Approved by the PCA Board on November 19, 2024

Table of Contents

Rationale

Risk is a term used to describe circumstances that put an entity at risk of injury, loss, or danger. Risks are unpredictable events triggered by natural hazards or human activities, which can lead to physical damage or economic losses.

Risks can disrupt the effectiveness of programs and projects specifically designed to uplift the lives of stakeholders, including employees, partner institutions, and beneficiaries. These risks manifest in many forms: weak operational strategies, economic instability, volatile trade and market policies, and heightened vulnerability to natural disasters.

Given this exposure, a Risk Management Plan is a vital and proactive strategy to safeguard an organization's objectives, operations, and resources. It offers a structured process for identifying, evaluating, and mitigating potential threats. This minimizes the adverse effects of risks on both daily operations and long-term goals.

In accordance with Administrative Order No. 119, s. 1989, all government offices, agencies, Government-Owned or Controlled Corporations (GOCCs), and Local Government Units (LGUs) are mandated to comply with the National Guidelines on Internal Control Systems (NGICS). The NGICS outlines essential principles aimed at guiding agencies to deliver public services that are economical, efficient, and effective[1].

A key provision under Section 3.2 of the NGICS requires agencies to incorporate risk assessments into their programs. This process helps identify, assess, evaluate, and mitigate internal and external factors that may threaten the achievement of an agency's strategic objectives. Effective risk management reduces the agency's exposure to uncertainties, enhancing operational efficiency.

Additionally, Executive Order No. 605, s. 2007, institutionalizes the Government Quality Management Program, which aligns with the International Organization for Standardization (ISO) 900 series, particularly the Quality Management Systems. This framework emphasizes the importance of developing loss prevention and mitigation plans to ensure that agencies meet their strategic goals and objectives.

Specifically, Clause 6.1 of ISO 9001:2015 requires organizations to identify both external and internal issues relevant to their strategic direction, assess risks in relation to stakeholder needs, and identify opportunities arising from these risks. By addressing these factors, organizations can reduce or eliminate existing and potential risks, thereby strengthening the effectiveness of their quality management systems.

A risk management plan is not just a tactical response to potential dangers; it is a strategic investment in the organization's future. By anticipating and proactively addressing potential threats, the organization protects more than just its immediate assets—it lays the foundation for sustainable growth and success.

Organizations face a wide range of hazards in today's complex and rapidly changing sector, from operational inefficiencies and regulatory compliance issues to financial instability and market changes. If these risks are not managed, they have the potential to impair stakeholder trust, interfere with regular operations, and even endanger the organization's sustainability. An effective risk management strategy enables the organization to:

1 **Secure Organizational Assets**

Risk management ensures the protection of an organization's most critical assets—its finances, infrastructure, intellectual property, and reputation. By identifying and assessing potential threats, the organization can implement targeted controls and safeguards to reduce its vulnerability to financial loss, physical damage, or reputational harm. This proactive approach provides a safety net, allowing the organization to recover more swiftly when risks do arise.

2 Drive Operational Efficiency and Performance

A key benefit of risk management is that it fosters operational efficiency. By minimizing the likelihood of unexpected disruptions, organizations can focus on their core objectives without constant interruptions. Furthermore, by identifying risks early on, organizations can avoid the costly repercussions of being reactive—such as damage control, loss of productivity, or expensive legal battles. This ensures streamlined operations and reduced inefficiencies, leading to more effective performance.

3 Enhance Decision-Making Processes

Risk management also serves as a foundation for informed decision-making. With a comprehensive understanding of the potential threats and opportunities, the management can make strategic choices with a clearer sense of the risks involved. This realization gives the organization more confidence to undertake necessary actions as it knows that the risks involved have been recognized, examined, and reduced. This allows the organization not just to avoid conflicts but also to execute better decision-making.

4 Ensure Compliance and Legal Protection

Organizations are required to comply with all legal and regulatory requirements. A strong risk management plan ensures that the organization remains compliant with these rules, reducing the chances of facing legal challenges or regulatory penalties. This protects the organization's integrity, preventing potential reputational damage and additional costs that may be incurred from legal liabilities.

5 Build Stakeholder Confidence

By demonstrating a commitment to risk management, organizations show they are forward-thinking, responsible, and capable of navigating uncertainties. This fosters confidence and enhances relationships with stakeholders, who are more likely to trust organizations that can manage crises effectively and maintain stability in uncertain times.

6 Build Resilience for the Future

Organizations need to be resilient and adaptive in a world where risks are rapidly changing as a result of technological advancements, climate change, and geopolitical instability. A robust risk management plan enables the organization to not only survive but thrive in the face of such challenges. By continuously monitoring and revising risk mitigation strategies, the organization becomes more responsive and better equipped to respond to both known and emerging threats.

Given the key aspects that the risk management plan covers, it is understood that it is more than just a safety measure, rather a strategic enabler of long-term success. By foreseeing and addressing potential challenges, the plan ensures the protection of assets, drives operational efficiency, supports informed decision-making, guarantees regulatory compliance, and strengthens trust with stakeholders. Ultimately, it equips the organization with the resilience it needs to navigate an ever-changing risk landscape, laying the groundwork for sustained growth and success well into the future.

Objectives

The Risk Management Plan aims to develop and implement an effective and pro-active response to the situation, perform risks assessment, develop strategies to mitigate risks using the available resources of the Authority.

Primarily, it aims to:

1. Identify and assess potential problems/risks;
2. Develop a risk management system to ensure that the PCA's strategic goals and objectives are achieved;
3. Ensure possible hazards/risks are reduced or eliminated by establishing control measures; and
4. Effectively monitor and evaluate of risk to ensure efficiency and effectiveness of operations and programs

Definition of Terms

- Risk – The chance of something happening that will have an impact on organization's objectives
- Risk Source – Refers to any element, condition, or activity that trigger the risks
- Risk Assessment – The overall process of risk identification, risk analysis and risk evaluation
- Risk Management – The culture, processes and structures that are directed towards realizing potential opportunities, whilst managing adverse effects
- Risk Reduction – Actions taken to reduce the probability, negative consequences or both, associated with a risk
- Risk Treatment – The process of selection and implementation of measures to modify risk
- Risk Appetite – Amount of risk PCA is willing to accept in pursuit of value
- Risk Tolerance – Readiness to bear the risk after treatment to achieve objectives
- Risk Severity – Gravity or magnitude of the impact
- Risk Probability – Likelihood of the frequency of occurrence of risk

Risk Management Process

Risk Management Cycle

Figure 1. Risk Management Cycle

There are five (5) basic steps in the Risk Management Cycle. The risk management cycle is a continuous process of identifying, assessing, treating, and monitoring existing and potential threats to an organization's objectives. It involves systematically identifying risks, evaluating its impact, and implementing strategies to mitigate or eliminate them. The cycle is continuous, requiring regular review and updates to ensure its effectiveness in safeguarding the organization's interests.

Implementation Strategies

Risk Management Process

Initiate Risk Evaluation

Start the annual risk evaluation process by reviewing the previous year's risk reports and current strategic objectives.

Responsible Unit / Person: Risk Assessment Office/Quality Assurance Head

Establish Risk Criteria

Define the Table Rating Criteria for Severity and Probability on a scale of 1 to 5.

Responsible Unit / Person: Risk Assessment Office

Identify Risks

Identify potential risks based on the organization's strategic goals and objectives.

Responsible Unit / Person: Deputy Administrators Regional Managers, Department Managers, Division Chiefs, Unit Heads

Assess Risks

Understand the risk's source and how it will affect the organization's implementation effectiveness and efficiency.

Responsible Unit / Person: Deputy Administrators Regional Managers, Department Managers, Division Chiefs, Unit Heads

Prioritize Risks

Prioritize risks to be addressed by deciding on the organization's Risk Appetite and Risk Tolerance.

Responsible Unit / Person: Deputy Administrators Regional Managers, Department Managers, Division Chiefs, Unit Heads

cont..

cont..

Validate and Document Risks

Ensure risks are correctly documented, adequate, complete, and conform to required formats.

Responsible Unit / Person: Risk Assessment Office

Identify Risk Management Strategies

Determine strategies or action plans to address identified risks.

Responsible Unit / Person: Deputy Administrators Regional Managers, Department Managers, Division Chiefs, Unit Heads

Implement Risk Management Strategies

Execute the risk management plan by implementing control measures to mitigate identified risks.

Responsible Unit / Person: Deputy Administrators Regional Managers, Department Managers, Division Chiefs, Unit Heads

Conduct Monitoring and Post Evaluation

Conduct monitoring and post-implementation evaluation to assess the effectiveness of the risk management plan and update records.

Responsible Unit / Person: Risk Assessment Office

Risk Evaluation

Risk evaluation will be done by reviewing the previous year's risk reports and current strategic objectives of the Authority. This may be done through SWOT analysis, stakeholder's consultation, and TWG meeting. The PCA's success indicators and strategic objectives shall be taken into consideration in risk evaluation to ensure alignment with overall goals.

Establishment of Risk Criteria

The identified risks will be evaluated on two (2) dimensional matrix using a quantitative rating of the probability of the event occurring and the scale of the possible severity. The risk analysis provides information critical to determining the risks need to be treated and how to implement the identified action plans.

Table 1. Risk Probability Rating

Level	Adjectival	Description	Indicator
1	Rare	May occur in exceptional cases	May occur once in every 4 – 6 years
2	Unlikely	Could occur at some time	May once every 3 years
3	Moderate	Should occur at some time	May occur once every 2 years
4	Likely	Will occur in most circumstances	May occur once a year
5	Almost certain	Recurring risk	May occur more than once a year

Table 2. Risk Severity Rating

Level	Adjectival	Areas				
		Financial	Operations	Internal Process	Organization	Stakeholders
1	Insignificant	Minor financial loss (<5% of the budget)	Negative impact to < 3% of the total coconut population	Minimal disruption in the delivery of service within the working day	No violation of law, rule, or regulation	Minor adverse public attention or complaints
2	Minor	Low financial loss (5 to 10% of the budget)	Negative impact to 3 to 10% of the total coconut population	Disruption in the delivery of service causing delay for 1 - 3 working days	Written warning / notice	Minor adverse media attention
3	Moderate	Medium financial loss (11 to 20% of the budget)	Negative impact to 11-20% of the total coconut population	Disruption in the delivery of service causing delay for 4 - 7 working days	Reprimand of employees / officials	Heightened and/or significant adverse media attention
4	Major	High financial loss (21 - 40% of the budget)	Negative impact to 21 - 40% of the total coconut population	Disruption in the delivery of service causing delay for 8 - 20 working days	Violation of law, rule, or regulation resulting to minor penalty or fine	On-going serious public or media outcry (national coverage)
5	Catastrophic	Major financial loss (>40% of the budget)	Negative impact to >40% of the total coconut population	Disruption in the delivery of service causing delay for more than 20 working days	Serious violation resulting to penalty, fine, or imprisonment	On-going serious public or media outcry (international coverage)

Risk Identification

The risk identification process is the first step in the risk management cycle. It involves systematically identifying potential threats or events that could impact an organization's objectives.

Risks can be identified through various methods, including SWOT analysis, technical workshops, and group consultations. When identifying risks, it is crucial to consider the unit's success indicators and strategic objectives to ensure alignment with overall goals. The following are the different types or categories of risks to be assessed:

1. Financial Risks – This refers to risks that may disrupt the fiscal health of the agency.
2. Disaster Risks – This refers to external risks brought about by natural threats to the agency.
3. Technological Risks – This refers to risks on information technology, data or applications that negatively impact operations of the agency
4. Operational Risks – This refers to risks that may hamper or interfere daily operations and processes particularly in the implementation of the programs, projects and activities. This may be further subcategorized into regular operations, human resource, and health.
5. Regulatory / Political Risks – This refers to risks of failing to comply with laws, regulations, or standards relevant to the project or changes in government policies, or regulatory environments that will affect project operations.
6. Reputational Risks – This refers to the potential for negative public perception or loss of stakeholder trust due to actions, behaviors, or events that can harm the institution's image and credibility.

Understanding risk sources is crucial in developing an effective risk management plan. Risk sources are the origins or underlying factors that give rise to potential risks within an organization. In identifying risks, determining its sources helps in predicting, assessing, and mitigating risks more effectively.

In PCA's context of Risk Management Plan, two key sources of risks are identified: internal and external. Internal risks refer to those arising from within the organization that can be controlled or managed by the PCA. These include operational inefficiencies, delays in project implementation, misallocation of resources, or personnel issues that could hinder program delivery. On the other hand, external risks are beyond the PCA's direct control and stem from outside factors. These include natural disasters like typhoons, economic fluctuations, changes in government regulations, or market instability. Such external forces could disrupt project timelines or impact the livelihoods of coconut farmers, which are central to PCA's mission.

Shown below are examples of risks categorized by their sources.

Table 3. List of Sample Internal Risks

Type of Risk	Description	Examples
Operational Risks	Failures in day-to-day operations or processes that can affect the PCA's performance.	
Operations		Equipment failure, process inefficiencies, inadequate support and/or poor knowledge transfer to the program beneficiaries
Operations - Human Resource		High employee turnover, lack of skilled labor, or low employee morale.
Operations - Health		Unsafe working conditions

cont..

Table 3. List of Sample Internal Risks *(cont)*

Type of Risk	Description	Examples
Financial Risks	Issues arising from financial mismanagement or constraints.	Cash flow problems, budget overruns, poor financial planning, or poor investment decisions (incomplete or unfinished projects).
Technological Risks	Risks due to outdated or failing technology systems and infrastructure.	Software failures, cyberattacks, or inadequate IT systems
Regulatory / Political Risks	Internal guidelines and regulations not being strictly complied or changes in political landscape.	Non-compliance with a certain operational guidelines issued by the Management or discontinuation of a project upon change of leadership
Reputational Risks	Internal actions or failures that harm the organization's image.	Poor customer service, ethical violations

Table 4. List of Sample External Risks

Type of Risk	Description	Examples
Regulatory / Political Risks	Changes in political landscape, government regulations, or legal requirements.	New taxes, changes in trade policies, or stringent environmental regulations.
Technological Risks	Rapid changes in technology that affect industry standards or processes.	Technological advancements or use of automation system that the institution and/or its clients cannot fully / immediately adopt.
Disaster Risks	Natural or environmental events that could affect business operations.	Natural disasters (earthquakes, floods, storms), climate change, or pandemics.

cont..

Table 4. List of Sample External Risks *(cont)*

Type of Risk	Description	Examples
Reputational Risks	Actions, behaviors, or events that can harm an organization's image, credibility, or brand	Negative public perception or loss of stakeholder trust

Risk Assessment

Risk assessment involves understanding how potential risks could impact an organization's program operations and, to the extent possible, estimating its effects on stakeholders' incomes and livelihoods.

Risks will be assessed using the established criteria to evaluate the level of frequency and severity. The organization's risk appetite and tolerance levels will be taken into account, along with the capacity of key stakeholders—such as farmer groups and local government units—to manage the identified risks effectively.

Additionally, the level of existing control measures will be determined to take into account into the prioritization which risks require immediate action. This involves reviewing the current protocols, guidelines, and regulations already in place within the organization. By assessing these factors, PCA will be able to prioritize risks that pose the greatest threat and craft appropriate mitigation strategies to address them.

The ultimate goal of this process is to gain clear understanding of potential threats and their impact, allowing the organization to make informed, proactive decisions to protect both its programs and the stakeholders it serves.

Table 5. Level of Control

Level	Adjectival	Description
1	Low	No existing protocol or guidelines
2	Medium	Protocol is existing but needs to be improved, revised, updated, or reinforced
3	High	A protocol is in place to ensure data credibility, policy compliance, asset protection, budget utilization, and target achievement

Risk Prioritization

Once the risks are assessed and analyzed, along with its existing control measures, the next step is to prioritize them. This process is essential for making evidence-based decisions regarding priority investment areas and determining the appropriate strategic actions to address the risks.

Risk prioritization will be based on its frequency and severity, as well as the organization's risk appetite and tolerance. A two-dimensional matrix shall be used to evaluate and categorize these risks, color-coded according to its impact level on the organization. This visual tool helps identify which risks require immediate attention and which can be managed with existing controls, ensuring a focused and informed approach to risk mitigation.

The allocation of resources and the urgency of actions to mitigate risks shall be determined based on the risk level, ranked from highest to lowest as: High Risk, Significant Risk, Moderate Risk, and Low Risk. This structured approach ensures that the most critical risks, which pose the greatest threat to the organization's objectives, are addressed first, with appropriate resources and swift action. Lower-level risks will be managed accordingly, based on its potential impact, ensuring efficient and effective risk management across all areas.

Table 6. Risk Probability Rating

Probability	Severity				
	1	2	3	4	5
5	S	S	H	H	H
4	M	S	S	H	H
3	L	M	S	H	H
2	L	L	M	S	H
1	L	L	M	S	S

Legend:

- H – High risk; severe impact and are highly likely to occur, posing a major threat to operations or objectives
- S – Significant risk; significant impact and occur more frequently
- M – Moderate risk; moderate impact and a higher likelihood of occurrence
- L – Low risk; minimal impact and occur infrequently

Risk Validation and Documentation

This process shall be facilitated by the Risk Assessment Office to ensure all identified risks are thoroughly reviewed, validated, and accurately documented. This involves prioritizing risks based on their potential impact and maintaining a centralized system for tracking and monitoring. To support this, the unit will establish a Risk Identification, Treatment, and Action Registry (RITAR), which will provide a comprehensive record of each risk, its assessed impact, and the planned mitigation strategies. This registry will enable clear oversight and ensure that all risks are managed effectively and consistently across the organization. (See Annex A)

Risk Management Strategies

Once the level of risks has been determined, the responsible units will develop strategies or risk treatments. These treatments may involve tools, practices, or policies aimed at reducing or eliminating the identified risks. Below are the different types of risk treatments that will be adopted by PCA:

1. Risk Avoidance – Alter plans and/or processes to entirely avoid the risk.
2. Risk Sharing/Transfer – Shift the impact of the risk to another party
3. Risk Mitigation – Implement measures to minimize the likelihood or impact of the risk.
4. Risk Acceptance – Acknowledge the risk but chose proceed with the plan / operations, often when the cost of mitigation exceeds the risk's impact.

Table 7. Risk Treatment Strategies

Risk Level	Risk Treatment			
	Acceptance	**Mitigation**	**Share / Transfer**	**Avoidance**
H		Implement strategies after treatment from Share / Transfer is applied for the residual risks	Implement strategies after treatment from Avoidance is applied for the residual risks	• Immediate response required to eliminate risk or reduce impact • Change project scope / regulations or discontinue program/project • Report immediately to Top Management • Closely monitor until risk impact is managed or eliminated
S		Implement strategies after treatment from Share / Transfer is applied for the residual risks	• Develop and apply specific tools, practices, or policies to mitigate the risk. • Strengthen controls, revise workflows, or invest in new technology. • Develop contingency plans to prepare for potential incidents and reduce the impact of risk • Report to Top Management	
M		• Implement measures to reduce the likelihood or impact of the risk. • Improve internal processes, enhance resource allocation, or provide additional training • Regular monitoring to ensure the risk is managed or reduced • Report to Senior Officers		
L	• No immediate action needed • Monitoring and periodic reviews are needed to ensure the risk remains low.			

The responsible offices/units shall revisit their risk management templates and discuss the relevant mitigation plans with the corresponding cost of the solution. The date of implementation of each plan must be specified. The responsible units may also integrate recommendations from various stakeholders and develop a comprehensive risk management plan.

Implementation of Risk Management Strategies

The risk management plan, approved by the PCA Board, will be implemented across all PCA units to mitigate their identified risks. Each unit will be responsible for executing their specific risk management strategies that correspond to their risks within their respective areas.

Funding for these strategies will be charged against the corporate operating budget to ensure the effective implementation of the action plans. Allocations for the following year will be determined annually based on the results of the year-end assessment and evaluation, subject to fund availability.

To ensure continuous monitoring and accountability, all offices shall regularly update their respective Risk Identification, Treatment, and Action Registry (RITARs). This shall be submitted to the Corporate Planning Service (CPS) to track the progress and developments of the mitigation measures.

Post Evaluation and Review

The Risk Management Office, under the CPS, will facilitate the monitoring and review of reports to evaluate the effectiveness of the PCA's Risk Management Plan. The review shall focus on identifying the strengths and areas for improvement on the implementation. A post-implementation evaluation will be carried out to assess the overall impact and success of the risk management plan. The Risk Management Office shall present the evaluation's findings to the Management, to ensure that records and risk strategies can be updated, if necessary.

An annual review and planning activity will be conducted to continuously enhance the PCA's Risk Management Plan. This will help maintain and improve the organization's competency in risk management, ensuring that the Authority remains resilient and proactive in addressing emerging risks.

Annex A. Risk Identification, Treatment, and Action Registry (RITAR)

PCA-FM-CP-01-01
Rev. 2
01-July-2024

RISK IDENTIFICATION, TREATMENT, AND ACTION REGISTRY
Department of Agriculture
Philippine Coconut Authority

Registry as of _____
Branch / Region / Department _____

Strategy Measure	Risk Identification			Risk Assessment			Risk Treatment					Status of Action Plan	Monitoring
	Risk	Source	CL	P	S	RL	Risk Treatment	Action Plan	Responsible Unit / Staff	Timelines			
										Start	End		

Note: P - Probability; S - Severity; RL - Risk Level

Prepared by:

Focal Person

Reviewed by:

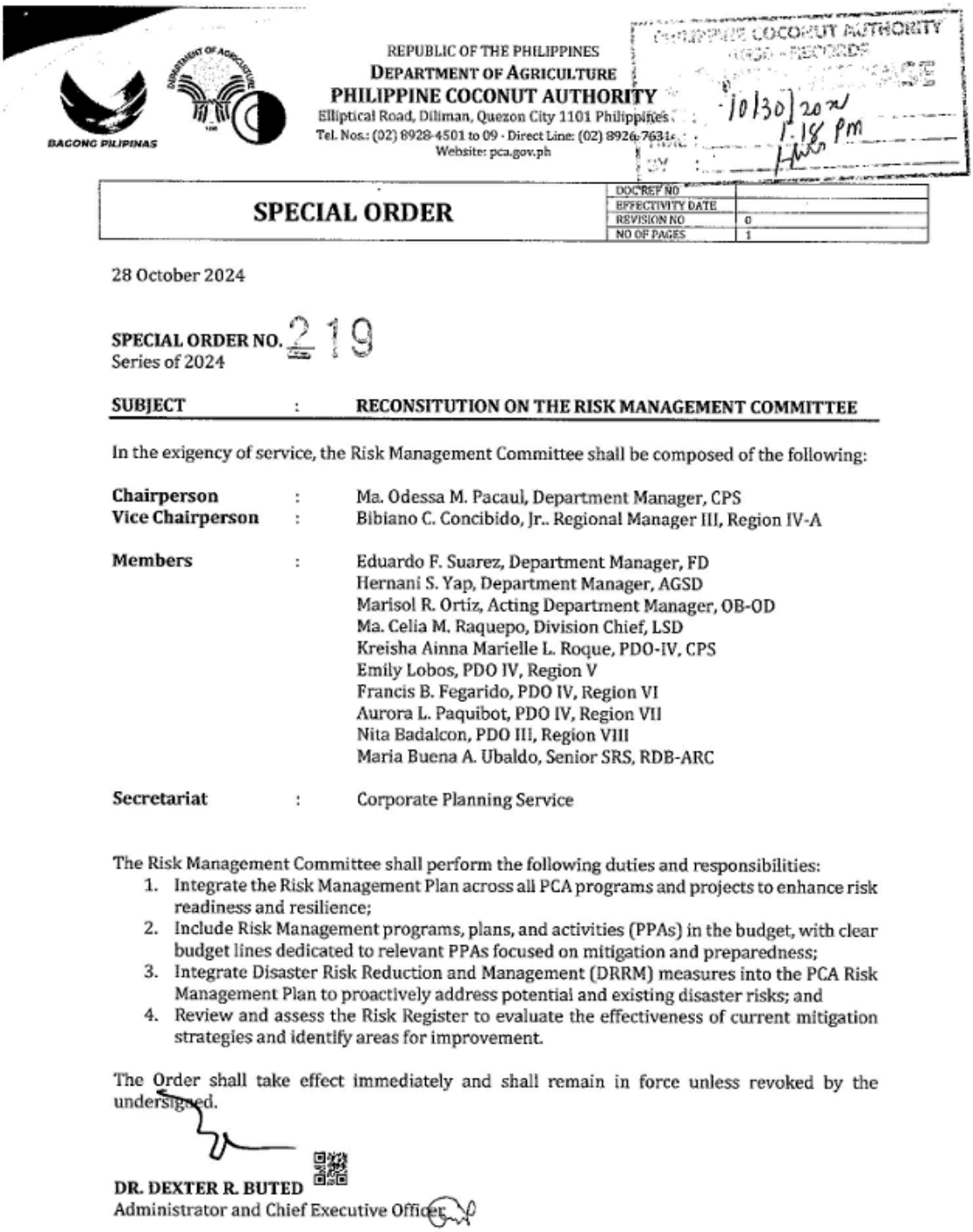
Senior Technical Staff / PDO IV

Noted by:

Regional Manager / Department Manager / Deputy Administrator

Annex

Annex B. Reconstitution of the PCA Risk Management Committee



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF AGRICULTURE
PHILIPPINE COCONUT AUTHORITY
Elliptical Road, Diliman, Quezon City 1101 Philippines
Tel. Nos.: (02) 8928-4501 to 09 · Direct Line: (02) 8926-7631
Website: pca.gov.ph

BAGONG PILIPINAS

PHILIPPINE COCONUT AUTHORITY
RECORDS
10/30/20
1:18 PM

SPECIAL ORDER

DOC REF NO	
EFFECTIVITY DATE	
REVISION NO	0
NO OF PAGES	1

28 October 2024

SPECIAL ORDER NO. 219
Series of 2024

SUBJECT : **RECONSITUTION ON THE RISK MANAGEMENT COMMITTEE**

In the exigency of service, the Risk Management Committee shall be composed of the following:

Chairperson	:	Ma. Odessa M. Pacaul, Department Manager, CPS
Vice Chairperson	:	Bibiano C. Concibido, Jr.. Regional Manager III, Region IV-A
Members	:	Eduardo F. Suarez, Department Manager, FD
		Hernani S. Yap, Department Manager, AGSD
		Marisol R. Ortiz, Acting Department Manager, OB-OD
		Ma. Celia M. Raquepo, Division Chief, LSD
		Kreisha Ainna Marielle L. Roque, PDO-IV, CPS
		Emily Lobos, PDO IV, Region V
		Francis B. Fegarido, PDO IV, Region VI
		Aurora L. Paquibot, PDO IV, Region VII
		Nita Badalcon, PDO III, Region VIII
		Maria Buena A. Ubaldo, Senior SRS, RDB-ARC
Secretariat	:	Corporate Planning Service

The Risk Management Committee shall perform the following duties and responsibilities:

1. Integrate the Risk Management Plan across all PCA programs and projects to enhance risk readiness and resilience;
2. Include Risk Management programs, plans, and activities (PPAs) in the budget, with clear budget lines dedicated to relevant PPAs focused on mitigation and preparedness;
3. Integrate Disaster Risk Reduction and Management (DRRM) measures into the PCA Risk Management Plan to proactively address potential and existing disaster risks; and
4. Review and assess the Risk Register to evaluate the effectiveness of current mitigation strategies and identify areas for improvement.

The Order shall take effect immediately and shall remain in force unless revoked by the undersigned.

DR. DEXTER R. BUTED
Administrator and Chief Executive Officer

Masaganang Agrikultura, Maunlad na Ekonomiya

References

Department of Agriculture. (2023). *Philippine Agriculture and Fisheries Extension Strategic Plan 2023-2028*. Manila, Philippines: Department of Agriculture.

Philippine Coconut Authority. (2018). *Risk Management Plan. Internal Document*.

Platform for Agricultural Risk Management (PARM). (2018). *Agricultural risk management: Practices and lessons learned for development*.

International Organization for Standardization. (2015). *ISO 9001:2015(en) Quality management systems – Requirements*.

Executive Order No. 605. (2007, February 23). *Institutionalizing the structure, mechanisms and standards to implement the Government Quality Management Program, amending for the purpose Administrative Order No. 161, s. 2006*.

Administrative Order No. 119. (1989). *National Guidelines on Internal Control Systems*.

PHILIPPINE COCONUT AUTHORITY
RISK MANAGEMENT PLAN