# DISASTER RISK MANAGEMENT MODEL FRAMEWORK (PAPU)

## 1.0 INTRODUCTION

In recent years, several natural disasters have taken place in Africa. These include earthquakes, floods, volcanic eruptions and landslides. These disasters have a potential for causing catastrophic losses and have increased the need to have a specific Disaster Risk Management Model Framework.

This Disaster Risk Model (DRM) model Framework will be used by PAPU member countries as a guideline for disaster prevention, reduction and management.

It is advisable that for more detail, use be made the booklet as provided by Universal Postal Union (UPU) Building Resilience - A Guide to Disaster Risk Management for The Postal Sector of 2016.

The DRM (called the Emergency and Postal Resilience by the UPU, since June 2022) is a combination of the terms defined herein below.

The framework shall provide for the strengthening of national disaster risk management structures and mechanisms to support improved disaster/emergency preparedness, response and recovery as well as the more effective integration of disaster risk considerations into organisations' planning and budgeting.

Malawi & Mozambique were tasked to develop the Disaster Risk Management Model Framework for PAPU Member States to be presented to the Strategy Committee (SC) in July 2022 in DRC for consideration, deliberation and adoption before approval by the Administrative Council during the same month in DRC.

The Disaster Risk Management model framework for the PAPU Member States will endeavour to highlight the steps that will be taken to avoid disruption of postal operations during an occurrence of a disaster.

Disasters come in different forms such as:

(i) Natural calamities cyclones, floods, and earthquakes which some countries such as in some countries such as Malawi, Mozambique, Zimbabwe etc. have experienced in the recent past;

(ii) Pandemics such as COVID-19;

(iii) They can also be in the form of conflicts, like war conflicts that happen within a country or across countries.

There are also government melt downs (wrong governance) – thus not being able to sustain the postal sector for example to point of dowse as a risk.

**2.0 TERMS**

Disaster - is an occurrence disrupting the normal conditions of existence and causing a level of suffering that exceeds the capacity of adjustment of the affected community.

Vulnerability - is a set of conditions that increase susceptibility to losses from the impact of natural hazards.

Risk – is the probability of harmful consequences or expected losses resulting from interactions between natural hazards and vulnerable conditions (a situation involving exposure to danger).

Management - the process of dealing with or controlling things or people.

Risk management - is the process of identification, analysis, and acceptance or mitigation of uncertainty in investment decisions (in the case of postal operations management).

Risk Management - is the process of identification, analysis and acceptance or mitigation of uncertainty to an organization's capital and earnings.

These threats, or risks, can include financial uncertainty, legal liabilities, strategic management errors, IT security threats (malware, unwanted access to sensitive data, etc.), accidents and natural disasters. Employees within the Risk Management Group are essentially responsible for evaluating all the risks the company faces, formulating responses and plans of action to mitigate and respond to those risks and making such plans of action available to all stakeholders, shareholders and potential investors (typically within the company's annual reports).

PAPU member countries must be encouraged to have a section that will be handling disaster risk management.

Risk assessment - is a process of identifying new competitors, data security issues, reputational or Public Relations (PR) risks, financial or liquidity risks, product recalls or even weather or natural disaster risks, among other things.

Risk Reporting - is a process tasked with defining the administration's data collection procedures (related to collecting information concerning potential risks and overall policy and employee compliance), creating clear and understandable reports and distributing them to Management.

Such reporting is often facilitated through risk management information systems and typically contains the risk profile for the organization (the most significant risks and why they are considered to be so, how such risks are being controlled, and any particular control gaps that are identified and how these are proposed to be filled), the changes in that risk profile since the last report and the performance of the risk management "system" or framework.

Framework - a basic structure underlying a system, concept, or text.

Disaster risk management - is the application of disaster risk reduction policies and strategies to prevent new disaster risk, reduce existing disaster risk and manage residual risk, contributing to the strengthening of resilience and reduction of disaster losses.

Disaster risk management actions can be distinguished between prospective disaster risk management, corrective disaster risk management and compensatory disaster risk management, also called residual risk management.

Prospective disaster risk management activities address and seek to avoid the development of new or increased disaster risks. They focus on addressing disaster risks that may develop in future if disaster risk reduction policies are not put in place.

Corrective disaster risk management activities address and seek to remove or reduce disaster risks which are already present and that need to be managed and reduced now.

Disaster risk management plans set out the goals and specific objectives for reducing disaster risks together with related actions to accomplish these objectives. They should be guided by the Sendai Framework for Disaster Risk Reduction 2015-2030 and considered and coordinated within relevant development plans, resource allocations and

programme activities. The postal-level plans need to be specific to each level of administrative responsibility and adapted to the different social and geographical circumstances that are present.

## 3.0 MISSION, GOAL AND OBJECTIVE

The mission of the framework is to be done through the five phases of the DRM which are:

(i) Prevention (P) - the action of stopping a disaster from happening or arising.

In DRM, risk prevention refers to the implementation of integrated measures to strengthen resilience through preventing new, and reducing existing, disaster risks, reducing the postal administration's exposure to hazards and vulnerability to disasters, and increasing preparedness for response and recovery.

(ii) Preparedness (P) - a state of readiness in case a disaster happens.

(iii) Response (R) - an answer to a disaster occurrence.

(iv) Recovery (R) - a return to a normal state of operations,

DO's Emergency Management Teams should always consider focusing their response and recovery activities on the following groupings (the" postal three Ps"):

- People –should safeguard the welfare of staff, contractors and customers by maintaining proper accounting for personnel, safety and security support, and the payment of wages and provision of benefits.
- Property – also maintains a viable infrastructure of processing, transportation, retail and delivery facilities as well as the equipment necessary to process, transport and deliver mail.
- Product – to ensure the viability of mail acceptance, processing and delivery.

In the postal three Ps, these include the following:

(a) People – employees, customers, customers

(b) Property – postal infrastructure and equipment/vehicle for acceptance, processing, transportation and delivery of mail; and

(c) Product – mail, stamps and stock.

(v) Mitigation (M) – make structural and non-structural changes to limit the impact of the disaster.

PPRRM's goal is to ensure a balance between the reduction of risk and the enhancement of postal operations resilience.

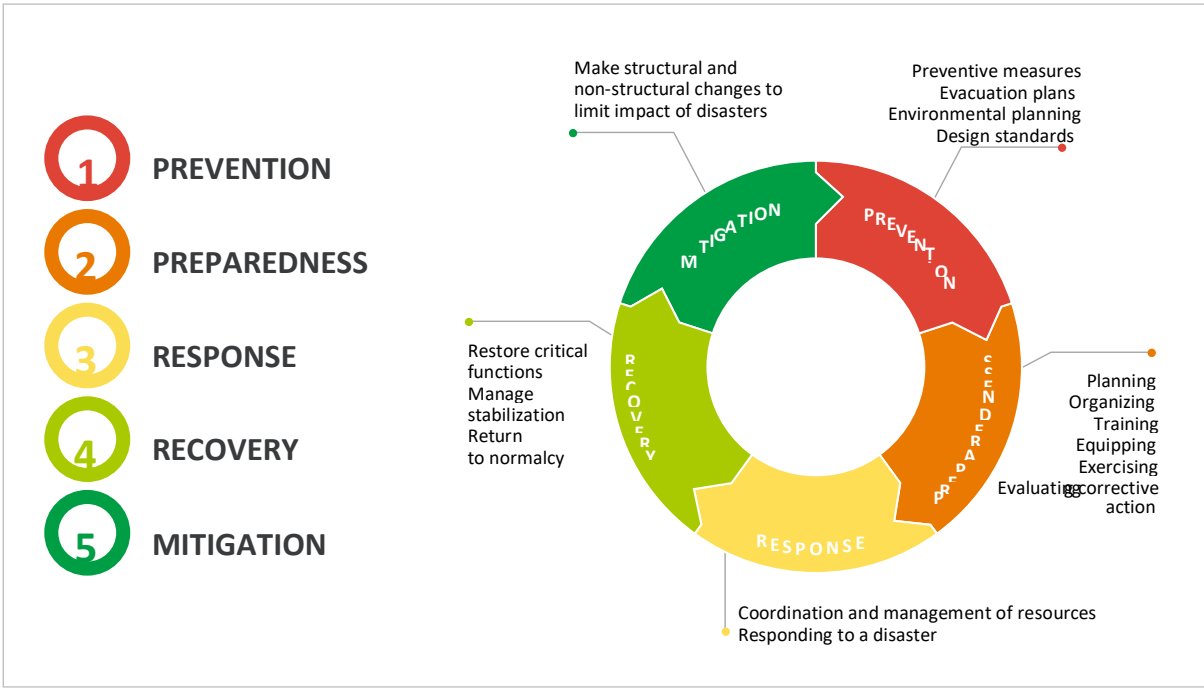
The objective of the framework will be to ensure:

(i) Effective response and

(ii) Recovery capabilities for designated postal operators in the PAPU Member States will enable them to deal with the effects of any form of disaster that may occur.

In short, the objective of the framework is to build on the established Disaster Risk Reduction practice of pro-actively strengthening prevention, mitigation, and preparedness activities (pre-disaster phase) and combine them through a management perspective with a response and recovery actions (post-disaster phase).

DRM activities are often grouped into five phases




## 4.0 OUTCOME OF DRM FRAMEWORK

The DRM framework will assist the PAPU Member States in the following ways:

(i) Identify potential disaster risks and manage actual ones;

(ii) Reduce the number of disaster-related risks;

(iii) Identify policies, responsibilities and procedures to protect staff and customers as well as effectively manage disasters (Annex I);

(iv) Promote understanding of disaster response program for staff for the PAPU Member States through training sessions;

(v) Establish operational concepts and procedures associated with responses to emergencies.

Additionally, the elements in the Disaster Risk Management Model framework will also include:

(i) The organisation's mission and the defined goals and objectives for the DRM Program

(ii) A vulnerability and risk assessment to include internal and external dependencies

(iii) Assessment of capabilities, skills, abilities, resources, obligations and authorities to develop plans and a management system

(iv) Engagement of senior management, key stakeholders and customers at the onset and throughout to reduce unforeseen consequences, including establishing and supporting working groups at the various levels of the organization.

(v) A realistic, flexible and adaptable DRM program that responds to the unique conditions of disasters and complies with security measures and requirements.

(vi) Standard policies, procedures, resources and tools

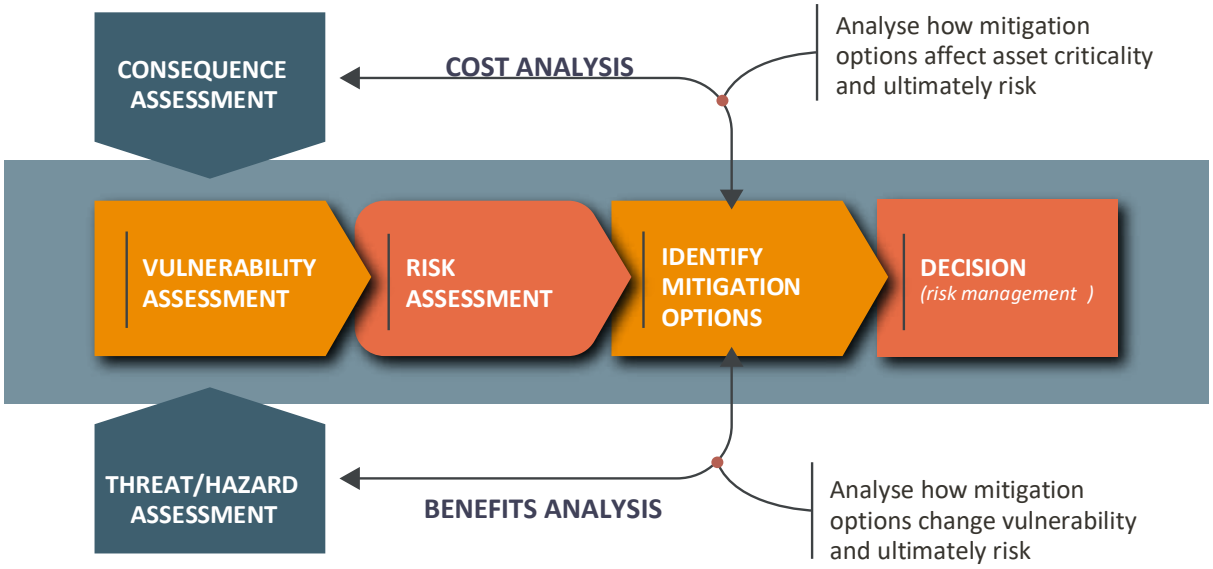
(vii) Integration of DRM and business continuity programs

(viii) Viable training and exercise plans

(ix) A framework for continual improvement and corrective action process for a fully viable life-cycle DRM program.

## 5.0 RISK ASSESSMENT PROCESS

Postal administrations will be required to follow the following process to identify the situation they are passing through:




## RISK REGISTER

A risk register is an information repository an organization creates to document the risks they face and the responses they're taking to address the risks.

In the risk register the following information may be included:

(i) Risk description - a statement is used to communicate the risk to the relevant stakeholders

(ii) Risk Owner -each risk should be owned by one person and that person should have the knowledge and skills to plan and execute risk responses.

(iii) Triggers - to indicate when risk is about to occur or that the risk has occurred.

(iv) Category - assigning categories to your risks allows you to filter, group, analyse and respond to your risks by category

(v) Probability risk rating - probability is the likelihood of the risk occurring. Consider using a scale of 1 to 10, 10 being the highest.

(vi) Impact risk rating - impact, also referred to as severity or consequence, is the amount of impact on the project. Consider using a scale of 1 to 10, 10 being the highest.

(vii) Risk score - the risk score is calculated by multiplying probability x impact. If the probability is 8 and the impact is 5, the risk score is 40.

(viii) Risk response strategies -strategies for threats include: accepting the risk, avoiding the risk, mitigating the risk, or transferring the risk. Strategies for opportunities include: accepting the risk, exploiting the risk, enhancing the risk, or sharing the risk.

(ix) Risk response plan or contingency plan - the risk owner should determine the appropriate response(s) which may be executed immediately or once a trigger is hit. For example, a risk owner may take immediate actions to mitigate a threat. Contingency plans are plans that are executed if the risk occurs.

(x) Fall-back plans - for some risks, you may wish to define a fall-back plan. The plan outlines what would be done if the contingency plan fails.

(xi) Residual risks - the risk owner may reduce risk by 70%. The remaining 30% risk is the residual risk. Note the residual risk and determine if additional response planning is required.

(xii) Trends – it is noted that if each risk is increasing, decreasing, or is stable.

## 6.0 CONCLUSION

The outlined above draft DRM model framework is being shared with members of the Working Group for comments before the Chairman submits it to the Strategy Committee (SC) at its meeting in July 2022 in DRC for adoption before approval by the 40th Ordinary Session of the PAPU Administrative Council.

**Annex I**

## DISASTER PROCEDURES CHECKLISTS

Format for preparing the Disaster Procedures checklists, both for the Headquarter (HQ), Regional Headquarters (RHQ) and post offices (POs), for the top risk *hazard-specific threat* in respect of respective postal administration.

Guidelines: Checklists for all three phases i.e., pre-impact (before 0 hours), during (0-48 hours) and post-impact phases (48+ hours) and for both HQ and Field Units are to be prepared.

Postal Administration:

Disaster, in brief:

A. Checklist for HQ/RHQ:

| Situation | Tasks |
|---|---|
| Initial Critical Actions prior to and during the event ( - 0 hours) | |
| | |
| | |
| | |
| | |
| | |
| Response Procedures (0-48 hours) | |
| | |
| | |
| | |
| Recovery Actions (48+ hours) | |
| | |
| | |
| | |
| | |
| | |
| | |

B. Checklists for POs:

| Situation | Tasks |
|---|---|
| Initial Critical Actions before and during the event ( - 0 hours) | |
| | |
| | |
| | |
| | |
| | |
| | |
| Response Procedures (0-48 hours) | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| Recovery Actions (48+ hours) | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |