



Technical Guidebook
**Post-Disaster
Recovery and
Response Plan
for Development
Finance Institutions**
Response Manual
Ecuador 2016

With the support of



Finanzas para el desarrollo

RED DE INSTITUCIONES
FINANCIERAS DE DESARROLLO

Technical
Guidebook

Post-Disaster Response and Recovery Plan for Develop- ment Finance Institutions

Response Manual
Ecuador 2016

With the support of

Cordaid 
investment management

CREDITS:

Content developed by:

Ligia Maria Castro Monge – International Consultant

Compiled and systematized by:

Yamile Pinto Guerrón – *Red de Instituciones Financieras de Desarrollo*

Collaborators and sources of information:

ESPOIR Foundation

The study “Exogenous Risk Management for Financial Institutions that serve the most Vulnerable Segments of the Population”; Technical Support Facility and Caribbean Technical Support Facility, June 2011

Edited by:

Yamile Pinto Guerrón – *Red de Instituciones Financieras de Desarrollo*

Translated by:

Peter C. Newton-Evans

Photographs:

Ecuadorian Public Media Image Bank

Publication for free distribution, Quito, Ecuador, August 2016

www.rfd.org.ec

Design and layout
Aquattro
info@aquattro.com.ec

A faint, light-colored map of the state of Alaska is visible in the background of the page, extending from the top right corner down towards the bottom left.

Table of Contents

1. Introduction	5
2. Systematizing the Process	6
3. Response Manual	7
3.1 STEP ONE – Organization and Impact Assessment	7
A. Organization	
B. Impact Assessment for Key Resources	
C. Security of Key Assets for Institutional Operations	
D. Immediate Actions	
3.2 STEP TWO – Customer Impact Assessment	14
A. Preparing a List of Potentially Affected Customers for Desktop Review	
B. Designing a Customer Survey and Planning Visits	
C. Customer Needs for Special Treatment and/or Additional Funding	
D. Determining the Financial Impact on Development Finance Institutions (DFIs)	
E. Preparing a Monitoring System	
3.3 STEP THREE – Planning the Response	18
A. Products and Services to be Provided at each Agency/Customer Service Center	
B. Reviewing and Fine Tuning Credit Policies to Protect and Stabilize the Portfolio	
C. Informing the Staff of Policies and Procedures to Implement	
D. Communication Program for External Customers	
E. Ensuring Liquidity	
3.4 STEP FOUR – Implementation and Monitoring	22
A. Daily Meetings with the Operational Crisis Management Team	
B. Trend Analysis	
C. Reassessing and Refining Strategies	
4. Conclusions	24
5. ANNEXES	27
6. Photographs	43

1. Introduction

The earthquake of April 16, 2016, with 7.8 on the Richter scale, affected primarily the Ecuadorian provinces of Esmeraldas, Manabi, Guayas, Los Rios, Santo Domingo de los Tsáchilas, and Santa Elena, killing 655 people and injuring 4,605, with 48 missing and more than 29,067 in shelters.¹

The National Secretariat of Planning and Development (SENPLADES) estimated damages at around US\$ 3,000 million (3% of the GDP), especially in real estate, streets and roads, and production facilities. This mainly affecting the commercial, tourism, transportation, agriculture, construction, and financial sectors, and initially generated an increase in unemployment and underemployment, with a consequent reduction in incomes, purchasing power, debt capacity, and ability to pay.

In the specific case of the financial sector, it had a direct impact on the liquidity, profits and solvency of financial institutions as a result of i) a rise in delinquency, ii) increased withdrawal of savings by affiliates, iii) greater provisions, and iv) a potential loss of assets.

In response to the above, the *Red de Instituciones Financieras de Desarrollo* (RFD), together with the Dutch Social Investor: CORDAID Investment Management BV, developed a project to establish a framework of strategies designed to i) reactivating the operations of development finance institutions, ii) mitigating the risks arising from the earthquake of April 16, 2016, and iii) taking advantage of the opportunities presented by reconstruction and rehabilitation of the affected areas.

¹ Report prepared by the Risk Management Secretariat's Technical Team (04/25/2016, 13:00).

Within the framework of project execution, one client of CORDAID Investment Management BV was selected to develop a Post-Earthquake Recovery and Response Plan. The selected organization was ESPOIR Foundation (www.espoir.org.ec).

The senior consultant for this process was Ligia María Castro Monge, an international consultant specializing in exogenous risk management.

2. Systematizing the Process

This Technical Guidebook seeks to provide guidelines and best practices based on actions taken and lessons learned while implementing the process and on the document funded by the Technical Support Facility and the Caribbean Technical Support Facility and published in 2011 (Exogenous Risk Management in Financial Institutions that Serve the most Vulnerable Segments of the Population).

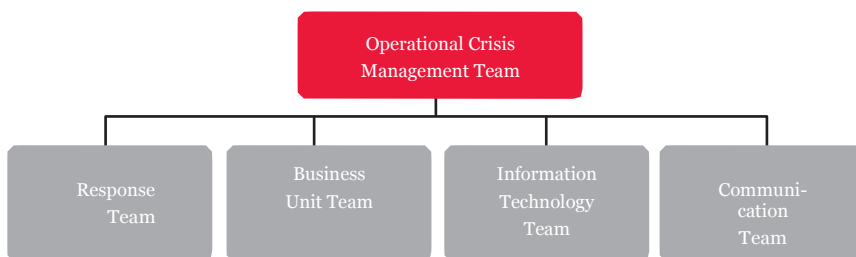
The recommendations contained herein are a roadmap for Development Finance Institutions (DFIs) to follow in the event of an exogenous disaster, whether natural, socio-natural or anthropogenic, that requires taking rapid but orderly, effective and efficient action.

3. Response Manual: Steps to Take

3.1 STEP ONE – ORGANIZATION AND IMPACT ASSESSMENT FOR KEY INSTITUTIONAL RESOURCES

A. Organization

The Operational Crisis Management Team, made up of senior officials, will be activated for overall management of a potentially disastrous incident, i.e., direction of activities during the emergency and recovery phases through a full understanding of the situation, the severity and extent of the problem, and the financial and non-financial consequences it has on the DFI. Sub-teams specializing in specific tactics will also be activated. These teams are part of the governance structure for the phase of activating the Business Continuity Plan (BCP) and should respond to whatever contingency scenario arises. These teams should have formally established roles and responsibilities related to emergency prevention and response. A typical response structure is as follows:



Below is a description of the institutions making up the Operational Crisis Management Team:

1. **Response Team:** A group of staff members to be convened immediately after an emergency in any geographic area where the organization works. It usually includes administrative, logistical and/or security personnel responsible for the recovery logistics (transporting materials and people, contacting suppliers, etc.).
2. **Business Unit Team:** Coordinates the activities of a specific post-incident business or functional unit and is responsible for ensuring recovery of critical procedures. It typically consists of line managers.
3. **Information Technology Team:** A group of specialists responsible for restoring technological infrastructure, communications, systems and/or data.
4. **Communications Team:** A specialized group to centralize release of information, define the most suitable communication channels and manage communications with customers and funders, depending on the type of contingency or incident.

The main activities of the Operational Crisis Management Team include:

1. Implementing the Business Continuity Plan (BCP)
2. Developing recommendations to address the crisis and policies to be adopted
3. Designing products and services to be offered to customers to stabilize the portfolio and liquidity
4. Communicating the policies to the staff and monitoring their activities
5. Analyzing crisis evolution on a daily basis

6. Coordinating communication according to the previously developed strategy and protocols (part of the BCP)
7. Retrieving and evaluating information on the impact on the DFIs and their customers
8. Developing financial and behavioral scenarios for liquidity, profits and equity
9. Negotiating temporary agreements with funders to avoid compromising institutional liquidity and for new financing as needed to meet targets in unaffected areas

B. Assessing Impacts on Key Resources

1. Initial Inventory of Key Resources

The key assets/resources are (i) human resources, (ii) plants and equipment, (iii) data, (iv) legal documents, and (iv) institutional procedures. To assess the degree of institutional impact, the following steps should be taken:

1.1 Security of Facilities

It is important to confirm the security and integrity of key institutional assets, prevent unauthorized persons from entering the premises to steal those assets, and ensure that they will not suffer additional damage due to natural causes.

Each agency/service center should be promptly contacted to understand their situation decide how to protect the institution's assets: additional security measures; transfer of staff, documents and equipment to another location; closing offices; or providing services from other agencies/service centers.

1.2 Impacts on Staff in Affected Areas

Knowing the effects a disaster has had on the staff in the affected areas is essential to determine the type of assistance the organization requires, such as food, medicine, shelter, counseling, etc. This matter should receive special attention, because in many disaster situations, an institution's officials may suffer similar losses to those of their customers. The degree of support the company provides to its personnel will determine their ability and motivation to continue serving customers during the difficult emergency, recovery and reconstruction stages.

Additionally, in the event of death, disability or absence of officials due to a catastrophic incident, determine the impact that such contingencies might have on the procedures and activities of the different departments, functional areas or agencies/service centers, in order to identify mechanisms or activate succession plans for the institution to continue operating as efficiently and effectively as possible in the post-disaster environment.

See the form in Annex 1: "Summary of Impacts on DFI Employees".

See the form in Annex 2: "Detailed Status of DFI Employees".

1.3 Damage to movable and immovable assets, and effect of replacement or reconstruction on cash flows and balances

As soon as possible, assess the impacts on the real estate that houses the agencies/points of service and determine the status of movable property to decide whether operations should be fully or partially reactivated at existing agencies/points of service or moved to other facilities, and whether new equipment should be purchased and/or the backup hardware activated.² Needless to say, for the assessment to be effective, the inventories of movable assets should be updated to facilitate information gathering.

The assessment findings will determine potential increases in operational costs and investments to ensure a return to pre-incident operating status and consequential impact of such actions on the cash flow and financial statements.

See the form in Annex 3: “Summary of Physical Damage to DFI Facilities”.

² Have a hardware backup contract in case of mass incidents to meet two objectives: (i) to expedite equipment supplies to the affected agencies/service centers, and (ii) to reduce the pressure on cash flow during the emergency period, allowing time for insurance companies to pay the compensation to purchase new equipment.

1.4 Impact of the Incident on Critical Procedures

The death or disability of officials and the destruction of physical infrastructure, equipment, documents, data, or information may impede or hinder the functioning of some procedures within the institution. Identifying affected procedures and the extent of any impacts on them is a task of paramount importance to activate the business continuity procedures (determine which to activate depending on the extent of any impacts).

2. Security of Key Assets for Institutional Operations:

Disaster impacts on databases, information systems, legal documents, and customer records could place significant restrictions on the institution's operations. Accordingly, in the first hours after the incident, you should:

- 2.1 Ensure that all computer equipment, communication links, information systems and main or alternate sites still work if within the affected areas. Similarly, confirm that data backups, on whatever media used (physical or virtual) are still operational, and if necessary use them to retrieve the information and/or applications.
- 2.2 Ensure that all legal documents on credits and all physical files on customers are in good conditions, protected by strict security criteria, and not exposed to subsequently damage or theft. Update and protect duplicate records and legal documents outside of the disaster zone.

2.3 Implement the business continuity plan, its disaster recovery plan, and the security plan for the technology area. These plans should be properly defined by each agency and/or service center, be up-to-date at the time of the incident and have undergone periodic testing and evaluation of results.

3. Immediate Actions

Based on the findings and conclusions of the assessments suggested in sections 1 and 2 above, DFIs should take immediate temporary measures to be set out in an effective Business Continuity Plan that is adapted to any potential risks that could affect the institution's critical procedures.

Among others, these measures should include agencies/points of service, personnel needs, business continuity procedures and methods, information and communication technology management, security and logistics, claims to insurance companies, communication strategies and plans for internal and external clients, international and local fund raising, etc.

If the disaster will create or increase levels of community insecurity, as part of business continuity procedures the DFI should supply the staff with security guidelines and train them in advance to implement those actions (as a preventive measure). The most important aspects to consider include:

- a. Remain alert, and if you suspect potential problems, immediately notify the community security authorities (police).
- b. Use clothing and shoes that allow ease of movement and the ability to run if necessary.
- c. Avoid traveling during hours of greatest danger (e.g., at sunset).
- d. Practice “security in numbers”, i.e., visit customers in groups of officials (2-4) to reduce risk.

3.2 STEP TWO – CUSTOMER IMPACT ASSESSMENT

Knowing what customers are going through and how this can affect the institution is vital to defining post-incident business strategies (loans, recoveries, financing, etc.) and to estimating the financial impacts of portfolio loss /deterioration, loan refinancing/restructuring and new loans. The inventory should answer at least the following questions:

1. How many customers’ homes are partially or totally damaged?
2. How many customers have had their businesses partially or totally damaged?
3. What percentage of the portfolio would be affected, and the source of the impact, e.g., inability to pay installments, loss of warranty, death of the customer, etc.?

4. Will customers require special treatment for outstanding loans (restructuring, refinancing) and/or additional funding for rehabilitation/reconstruction of homes and/or businesses?
5. How willing are customer to continue paying their installments on existing loans?

A. Preparing a List of Potentially Affected Customers for Desktop Review

- a. Using your databases, develop a list of customers in the affected areas.
- b. Estimate the risk portfolio of customers identified in the affected areas.
- c. Using the preliminary estimate of portfolio at risk, negotiate any arrangements/agreements needed to ensure your liquidity and plan the increase in provisions for deterioration of the loan portfolio.
- d. Ensure that each promoter and credit supervisor has the information on customers at risk (generated by the information system).

See the form in Annex 4: “Initial Estimate of Damages to DFI Customers”.

B. Designing a Customer Survey and Planning Visits

- a. Develop and systematize a survey document to assess the impact of the incident on each of the active customers located within the affected areas (loss of life, housing and/or business).
- b. Based on the information on customers developed by each promoter, plan the visit to the customers to apply the surveys.

- c. Develop an application to manage the information collected through the surveys.
- d. Assign personnel to input the survey information, and establish a mechanism to verify the quality of the information entered.

See the form in Annex 5 on “Type of Survey for DFI Loan Customers”

C. Customer Needs for Special Treatment and/or Additional Funding

Based on the information collected with the surveys, you can then:

- a. Project the number of customers who need their loans restructured, refinanced or rescheduled, and the portfolio amount this represents.
- b. Project the number of customers who will need auxiliary loans (new loans) and estimate the amount of their financial needs.
- c. Project the number of loans that may not be recoverable due to the death of the debtor and the guarantor’s inability to pay (under the assumption that the institution does not have debtor’s life insurance).

D. Determining the Financial Impact on the DFI:

Based on the survey findings on active clients and the projected customer demands for refinancing or new loans, the Operational Crisis Management Team will proceed to estimate or project:

- a. The credit risk of the post-disaster portfolio
- b. The impact of the disaster on recovery/collection, loan approvals, and fund disbursements
- c. Demand for new loans to meet customer needs
- d. Impact on income, expenses (financial, extraordinary, administrative, provisions, depreciation, etc.), profit, and financial position
- e. Resetting provisions and impact on indicators of expense provisions and risk portfolio coverage
- f. Liquidity requirements to address the direct and indirect impacts of the disaster to determine whether the DFI can cope with those impacts using its own funds, since it has no access to contingency/emergency liquidity lines, or whether it should consider requests to restructure, re-finance or reschedule its debts through international and/or local sources.

E. Preparing a Monitoring System

In times of crisis, normal monitoring systems are insufficiently robust. The data analysis and monitoring period should be shortened, and the effect of measures on the organization's financial health should be measured on a daily basis. A monitoring system is essential to compare normal scheduled daily flows (pre-disaster) with the current flows recorded (post-disaster).

3.3 STEP THREE – PLANNING THE RESPONSE

A. Products and Services to be Offered at each Agency/Service Center

Decide on the products and services to be offered at each agency/service center in the affected areas, depending on the degree of impact/damage to both the DFI and its customers.

B. Reviewing and Fine-Tuning Credit Policies to Protect and Stabilize the Portfolio

Many financial institutions, being unprepared to face a disaster (not having an effective, proven, tested business continuity plan), are thrown into chaos, respond sluggishly and provide untimely outcomes that arrive too late to effectively support customers at the most critical point of the emergency. Therefore, a good response plan should include credit policies for special cases of customer business disruption due to natural, socio-natural or anthropogenic incidents.

1. Writing off Debts

Debt relief should not be granted for any reason, as in the long run this practice undermines the customer commitment to pay and causes losses for the institution. Only in extreme cases, where a debtor has died because of the disaster, had no credit life insurance, and recovery through the guarantor is impossible, should DFIs write off a loan.

2. Loan Restructuring

Restructuring policies tend to be positive to prevent portfolio losses in scenarios where customers affected by a disaster are unable to meet payment schedules agreed to in the pre-disaster situation. It is hard to determine the optimal restructuring characteristics *a priori*. The most effective is a case-by-case approach, as this enables aligning the terms and conditions to the particular needs of each client.

However, past DFI experience with credit products designed and implemented in response to such incidents could lay the groundwork for the future. Thus, in the case of a new disaster, once its particular features (e.g., scope and breadth of impact) are known, the credit parameters used for response in the past can be adjusted and adapted based on a review of the type that will ensure the DFI enough funds to implement the chosen policy and to model the impact of the selected strategy on its financial and equity position.

The terms and conditions of the restructured loans should conform to the realities of the disaster area and consider, *inter alia*, the following: (i) scope and severity of the disaster, (ii) time of the disaster, (iii) community cash flow patterns, (iv) alternative sources of family income (employment or remittances), and (vi) the institution's liquidity.

3. Emergency Loans

Immediately following a natural disaster, a DFI can grant loans to help its customers survive the post-disaster emergency period (buying food, drinking water or medicines). These loans should be small, have a short repayment term (adapted to the nature of the incident and the reactivation of income generation), and be granted at zero interest or at a subsidized rate.

4. Loans for Reconstruction

This type of product is intended to enable customers to recover during the post-disaster period. It is meant to help households rebuild their standard of living by restoring homes and recovering assets to pre-disaster conditions. In general, the terms and conditions of these loans should reflect the income-generating potential of the assets to be financed and the customer's ability to pay, considering the damage caused by the disaster. The most advisable policy is to provide new loans **only** to customers with good credit records and indebtedness below a given critical level. These loans are more effective when granted once the reconstruction phase has begun (after the emergency phase has passed).

C. Informing the Staff of Policies and Procedures to be Implemented

All staff should be informed and aware of the policies and rules to govern the crisis period to convey them clearly, coherently and consistently to customers. It is advisable to prepare a memo with the key points, distribute it among all staff members and conduct on-site training for personnel.

D. External Customer Communication Program It is important for customers to know and understand the policies, rules and procedures to be applied. A note can be posted in the mass media (radio, newspaper, TV), or disseminated using vehicles with loud speakers. A “Customer Notice” can also be placed in conspicuous places at each agency/service center, clearly announcing the institution’s policies, rules and measures regarding its services to and relations with the public.

F. Ensuring Liquidity to Address the Drop in Loan Recoveries, New Loans, Payment of Financial Obligations and Incremental Expenses

The combined effect of reduced recovery and increased outlays for new loans (normal for unaffected areas plus emergency and reconstruction), together with paying financial obligations according to agreed schedules (until a refinancing agreement is reached with domestic and foreign funders), increased savings withdrawal, and growth in operating expenses and investments, (administrative, equipment and infrastructure recovery, logistics, staff overtime, etc.) can leave the institution in a significant liquidity crisis.

Therefore, a DFI should have a strategy for managing assets and liabilities to provide it sufficient liquidity to meet its own needs and those of its customers. Consequently, as part of business continuity plan, the DFI should have concrete (and negotiated) strategies and tactics to gain access to liquidity from various alternative sources: (i) special cash reserves (voluntary), (ii) agreements/arrangements for pre-approved credit lines with domestic and foreign financiers for rapid disbursement, (iii) keeping a non-disbursed amount of normal financing available for emergency cases, and (iv) participating in the money market to obtain funds for terms of up to 180 days, among others.

3.4 STEP FOUR – IMPLEMENTING AND MONITORING

The programs and policies adopted by the DFI should be implemented in an effort to return to normal as soon as possible. During this period, daily monitoring is what will ensure success.

A. Daily Meetings with the Operational Crisis Management Team

The Operational Crisis Management Team, as the body responsible for overall management of a potentially disastrous incident, should meet each morning to review the data, identify problems and decide what actions to take.

The data it will need to receive are:

1. Daily Report on the age of overdue balances
2. Recoveries from the day before compared to those scheduled (pre-disaster), and those accrued up to the day before compared to scheduled recoveries accrued.
3. Actual income and expenditure compared to schedule (pre-disaster), both for the day before and accrued up to the day before.

4. Actual disbursements compared both to those scheduled for the day before and to those accrued until the end of the day before.
5. New loan applications compared to those scheduled pre-disaster, for both the day before and accrued up to the end of the day before.
6. Customer requests for special consideration by both number and type of application.
7. Comments on the status of customers in the affected areas from branch managers, regional coordinators, loan supervisors, loan promoters, and other field staff.

B. Trend Analysis

The Operational Crisis Management Team should review the evolution of the key indicators and determine the implications of trends on a daily basis to answer one essential question: Is the situation improving or deteriorating?

Based on the daily data review, the Operational Crisis Management Team may, if necessary, re-estimate the magnitude of the problem the DFI faces and determine where to focus its response actions.

C. Reassessing and Refining Strategies

At least once a week, the Operational Crisis Management Team will need to analyze the trend review findings to reassess and refine its strategies, especially those relating to loan recovery and delinquency management, loan restructuring, payment or restructuring of financial obligations, additional financing requirements, provisioning, managing assets and liabilities to meet the institution's liquidity needs, and behavior of income and expenses.

4. Conclusions

In conclusion, it is important to mention the “Keys to Success in Exogenous Risk Reduction”³ as a prerequisite for adopting and implementing a comprehensive external risk management plan:

- **Corporate Governance:** Creating a culture of risk management in a broad sense should start at the highest levels of decision-making and institutional responsibility, and filter down.
- **Participation:** Building and implementing a culture of exogenous risk reduction and the plan designed to this effect should be highly participatory and involve all levels of the DFI, even at the highest level of corporate governance.
- **Recovery of Experiences and Monitoring:** Referring to past experience is an effective exercise to build institutional awareness. Knowledge of past incidents enables a DFI to conduct a cost-benefit analysis of operating with or without an exogenous risk reduction plan and to take action towards building a portfolio based not merely on criteria quantity and market share, but also on criteria of quality and the reduction of exposure and vulnerability to exogenous risks.

3 *Exogenous Risk Management in Financial Institutions that Serve the most Vulnerable Segments of the Population*, Technical Support Facility and Caribbean Technical Support Facility, Ligia Castro Monge, Costa Rica, 2011.

- **Using Installed Capacity:** Anchoring the design and development of an exogenous risk reduction plan to existing procedures and bodies helps to ensure the plan’s medium- and long-term sustainability and to keep it alive and under periodic review.
- **Prioritizing Efforts:** Once a DFI has identified its risk exposures and vulnerabilities, it should analyze the likelihood and expected impacts of the various risks in order to assess their impact on its medium- and long-term sustainability. It will then be able to prioritize the measures to be taken and to allocate the available funds as best possible.
- **Organizing for Business Continuity:** The DFI should have a governance structure that involves the Executive Directorate responsible for directing the development and management of the Business Continuity Plan (BCP) and strategies for continuity of critical business procedures. The Executive Directorate should be supported by a Business Continuity Management Committee. In addition, an Operational Crisis Management Team should be established to manage crises through sub-teams specializing in specific recovery tactics.

See Annex No. 6 – Business Continuity Management, Planning and Structure

- **Access to existing Information, Experience, Tools, Materials, and Resources:** It is extremely important to access and retrieve documentation that will facilitate internal actions and guide decision-making. A list of basic materials might include (i) threat maps for different geographical areas, (ii) risk zoning studies, (iii) disaster prevention, mitigation and relief plans, (iv) training materials and programs developed by authorities specialized in the emergency and disaster prevention and relief, and (v) specific studies on threats, risks and disasters in the DFI’s areas of operation.

- **Consultation and Coordination:** Once internal goals have been set and the resulting needs have been met, it is important to identify institutions to consult and coordinate activities to take advantage of existing resources without duplicating efforts, which involves establishing partnerships with entities specializing in disaster prevention, preparedness and relief.
- **Communication and Integration of Customers and Communications:** This variable should be present in both prevention efforts and operational emergency management. It helps develop a culture of prevention, enhances the institutional profile by bolstering customer security, and increases customer confidence in case of an emergency.

5. Annexes

ANNEX 1

SUMMARY OF DFI EMPLOYEE STATUS

[illegible]

ANNEX 2

DETAIL OF DFI EMPLOYEE STATUS

Office (national, regional or agency): _____					Date: _____		
Summary: _____ Total number of staff _____ No. of deceased employees _____ No. of employees with injuries (who can return to work) _____ No. of employees with serious injuries (unable to work) _____ No. of employees with deceased or injured relatives Assistance needs for staff and their families: Accommodation: for _____ families (number) Food and water: for _____ families (number); _____ individuals (number) Clothing: for _____ families (number); _____ individuals (number) Beds: for _____ families (number); _____ individuals (number) Financial aid: for _____ employees (number) Others: _____					Comments: 		
Detail for each official of damaged offices:							
Name	Position	Degree of damage suffered by employee			Number of wounded or deceased relatives	Other Damages	Needs
		Minor Injuries	Serious Injuries	Death			

ANNEX 3

SUMMARY OF SERIOUS PHYSICAL DAMAGES TO DFI FACILITIES

Type of Property or Infrastructure	Extent of Damage			Required Action	Estimated investment to recover property and infrastructure to its original condition (US\$)
	Slight	Medium	Severe		
National Office					
Physical structure (walls, ceilings, etc.)					
Utilities (water, electricity, sewage)					
Vehicles					
Communications (phone, fax, radio, cell phones)					
Computer systems (hardware, software)					
Legal documents and partner records					
Others					
Regional Office xxx (repeat for each regional office affected)					
Physical structure (walls, ceilings, etc.)					
Utilities (water, electricity, sewage)					

Type of property or infrastructure	Extent of damage			Required action	Estimated investment to recover property and infrastructure to its original condition (US\$)
	Slight	Medium	Severe		
Vehicles					
Communications (phone, fax, radio, cell phones)					
Computer systems (hardware, software)					
Legal documents and partner records					
Others					
Agency yyy (repeat for each affected agency)					
Physical structure (walls, ceilings, etc.)					
Utilities (water, electricity, sewage)					
Vehicles					
Communications (phone, fax, radio, cell phones)					
Computer systems (hardware, software)					
Legal documents and partner records					
Others					

ANNEX 4

INITIAL ESTIMATE OF DAMAGE TO DFI CUSTOMERS

Regional Office/Agency (a)	Total (number or amount)		Affected (number or amount)		Percentage of impact	
	Customers (b)	Portfolio US\$ (c)	Customers (d)	Portfolio US\$ (e)	Customers (100% * d/b) (f)	Portfolio (100% * e/c) (g)
TOTAL						

ANNEX 5

MODEL FORM FOR CREDIT CUSTOMER SURVEY

CREDIT CUSTOMER SURVEY

Agency: _____

Customer name				
Name of credit sponsor		Name of credit supervisor		
Business address (pre-disaster)		Business address (post-disaster)		
Business activity (pre-disaster)		Business activity (post-disaster)		
Home address (pre-disaster)		Home address (post-disaster)		
Household Situation				
No. of persons living at home	TOTAL	Children (under age 12)	Adults (over age 12 up to age 65)	Senior citizens (over age 65)
No. of persons impacted at home	TOTAL	Children (under age 12)	Adults (over age 12 up to age 65)	Senior citizens (over age 65)
Number of deceased	TOTAL	Children (under age 12)	Adults (over age 12 up to age 65)	Senior citizens (over age 65)
Number disappeared	TOTAL	Children (under age 12)	Adults (over age 12 up to age 65)	Senior citizens (over age 65)
Number of hospital-ized/disabled	TOTAL	Children (under age 12)	Adults (over age 12 up to age 65)	Senior citizens (over age 65)
Housing situation				
Degree of impact on homes	None	Partial	Total	
Degree of impact on furniture and household equipment	None	Partial	Total	
Degree of impact on other personal assets of those living in the home	None	Partial	Total	

Business Situation

Degree of impact on business establishment	None	Partial	Total
Degree of impact on equipment, furniture and inventories of finished goods and business supplies (for trade, food, manufacture, craft, and service activities)	None	Partial	Total
Degree of impact on crops, animals, equipment/tools, and infrastructure (irrigation, barns, storage systems, etc. for farming)	None	Partial	Total
No. of persons employed (pre-disaster)	Total	Relatives	Non relatives
No. of persons employed (post-disaster)	Total	Relatives	Non relatives
Impact on expected additional income	YES	NO	Describe

On loans in effect on date of the disaster

- Amount disbursed
- Total amount due (at time of disaster)
- Default due to disaster: YES _____ NO _____
- Days in arrears (at time of disaster)
- Number of installments in arrears (at time of disaster)
- Total amount of arrears/amount at risk (at time of disaster)
- Special remarks on customer credit behavior

Possibility to reactivate the business (term)

- _____ Active business
- _____ Up to 1 month
- _____ From 1 to 2 months
- _____ From 2 to 3 months
- _____ Over 3 months
- _____ Possibility of recovery only if additional funding is granted
- _____ No possibility of recovery, even with funding

Possibility of reactivating the business (term)

- _____ Catch up within 1 month
- _____ Catch up from 1 to 3 months
- _____ Catch up from 3 to 6 months
- _____ Difficult to recover

ANNEX 6

BUSINESS CONTINUITY MANAGEMENT, PLANNING AND STRUCTURE

Developing a business continuity plan (BCP) and strategy is a complex task that involves all levels of an organization, its procedures and activities. It cannot be developed solely by an outsider who is unfamiliar with the institution's daily operations. ***Business continuity is everyone's job!***

This section proposes a methodology to enable a DFI to develop a strategy and a BCP adapted to its own institutional features.

The ISO 22301 standard defines business continuity as:

“...the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.”

The ISO standard clarifies that business continuity management is not limited to information technology. Rather, it is *“a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.”*

In short, the BCP is a management and planning tool for addressing undesirable business disruptions (prevention and immediate response). It should guide and coordinate recovery of **all** critical business procedures and ensure the integrity of the organization's personnel and assets. Being a factor of managerial success, it should follow the dynamism and evolution of the organization (i.e., respond to the creation/elimination of business units, transformations in the organizational structure, amendments to internal or sectoral regulations, changes in technological infrastructure (hardware and software), changes in the organization's strategies, etc.)

Developing a BCP requires working at three levels:

1. Board of Directors/Executive Directorate: Define the Operational Continuity Policy, i.e., the desired general guidelines and problem-solving style on which the operational continuity procedures will be based.
2. Operational Departments: Establish the procedures to recover the basic operations of each department, based on the guidelines established by Senior Management.
3. Technology Department: According to the needs identified by the operational departments (procedures), it defines the technical strategies to regain the technological environment for each solution proposed.

Building a BCP requires assessing the organization in terms of its goals, how it operates, and what restrictions are imposed by its working environment.

1. Analyzing Business Impacts – Business Analysis and Risk Assessment

- i. Identify and prioritize critical procedures, set terms for recovery and tolerance levels for disruption of procedures. Prioritization of critical procedures can be based on potential loss of income and the severity of the impacts that the disruption would have. For example, for a DFI, the treasury and its procedures may be critical (collecting loans, paying bills and salaries, paying financial obligations, investing surplus, disbursing funds, etc.). By definition, all these procedures are critical to the daily operations of the DFI.
- ii. Establish a set of possible causes for contingencies, defined as situations that disrupt the organization's normal operations or compromise their levels for longer than is defined as permissible/tolerable, which cannot be solved using standard procedures. Potential contingencies include earthquakes, fires and floods, strikes, protests, vandalism, death or illness of key personnel, epidemic / infectious disease affecting staff, cyberattacks, financial crises, bad publicity / reputational attacks, loss of data / information, etc.
- iii. For all potential contingencies, determine their impacts on critical procedures and set the time that each critical process could be unavailable before the impact on the organization is deemed severe, i.e., the critical recovery time before suffering significant losses.

- iv. Determine the internal and external dependencies for each critical procedure, i.e., all types of critical internal and external resources needed to run those critical procedures. Internal: availability of human resources, applications, data/information, equipment/tools, and support services (financial, human talent, security, technical support, logistics, legal counseling). External: applications, data/information, equipment/tools, communications, utilities, legal services, financial institutions, insurance companies, health and safety services).

2. Business Continuity Plans – Recovery Strategies and Alternatives in Case of Disruption

- i. Identify scenarios that take into account the availability or lack of critical resources at incremental levels of severity of a disruption. Review the costs and benefits of different continuity options and select the most realistic, effective alternative for each critical process.

A good business continuity plan includes a disaster recovery plan. However, a disaster recovery plan in itself is not a business continuity plan.

Kyriba. Business Continuity Planning: why Treasury needs a Plan B. Treasury in Practice Series. Issue 10, March 2016.

- ii. Focus actions and prepare procedures to ensure the operations in each scenario – prepare contingency /response/recovery plans to ensure continuity based on the findings of the business impact assessment. The response will differ according to each incident and the disruption caused. A BCP is needed for each critical process, including existing continuity provisions in the organization that have proven to be effective and cost-efficient.
- iii. Define the teams that will lead and support the recovery and response operations, including their membership and authority structures, tasks and responsibilities, contact lists, and alternate members.
- iv. Availability of an alternate site, in case the main site or the assets, networks and technology applications are lost.

3. Preparation:

Successful implementation of a BCP requires socialization throughout the organization, to make all staff aware of the responsibilities they should assume upon activation of the continuity solution, and the roles that other officials/teams will play. A key element is drills/simulations that test the organization's preparedness to implement the BCP, including its capacity for institutional response to a risk incident, its effectiveness and response times, improved design and implementation mechanisms, quality and effectiveness of procedures for response and recovery, the staff's familiarity with the operational continuity solution, and other awareness-building and training needs.

4. Quality Assurance:

Once back to normal, each team prepares a report of the actions taken and its fulfillment of the BCP, the time and resources used, any difficulties encountered, recommendations to improve the procedures, etc., in order to adjust the BCP based on the lessons learned. In addition, BCP effectiveness and relevance should be assessed periodically (at least once a year) to identify opportunities for improvement through an internal or external audit.

5. Business Continuity Plan (BCP) Governance Structure

A BCP governance structure involves the Executive Directorate, responsible for steering the process of developing and managing the BCP and the strategies for the continuity of critical business procedures. The Executive Directorate should be assisted by a Business Continuity Management Committee. Additionally, an Operational Crisis Management Team should be established to manage crises through sub-teams specializing in specific recovery tactics.

Detailed below is a proposal for forming the institutions to govern the BCP and the duties of each one.

5.1 Executive Director – Duties

1. To assign the direction of the business continuity role to a Business Continuity Management Committee (see section 5.2).

2. To establish the Operational Crisis Management Team, comprised of key staff and functional managers of the critical operations areas, responsible for crisis management and business continuity during the crisis. The roles and responsibilities of each member should be clearly established.
3. To ensure that the BCP is aligned with the strategic plan of the institution
4. To allocate human and financial resources for BCP development and maintenance
5. To make policies regarding how to manage and monitor business continuity risks
6. To review the findings of the BCP tests regularly
7. To keep the BCP updated and to evaluate/review it at least annually
8. To ensure the staff has been trained and is fully aware of their roles in implementing the BCP
9. To develop a system for reporting BCP issues to the Board, which includes checking for appropriate awareness of the risks, mitigation measures and preparedness status
10. To ensure that the BCP undergoes an independent review (internal or external audit) at least annually
11. To ensure that the roles, responsibilities, authority to act and succession plans are clearly articulated in the business continuity policy to avoid confusion in the event of a disruption
12. To ensure that the BCP not only contemplates business procedures and technical/technological aspects, but also recognizes and addresses human factors

5.2 Business Continuity Management Committee

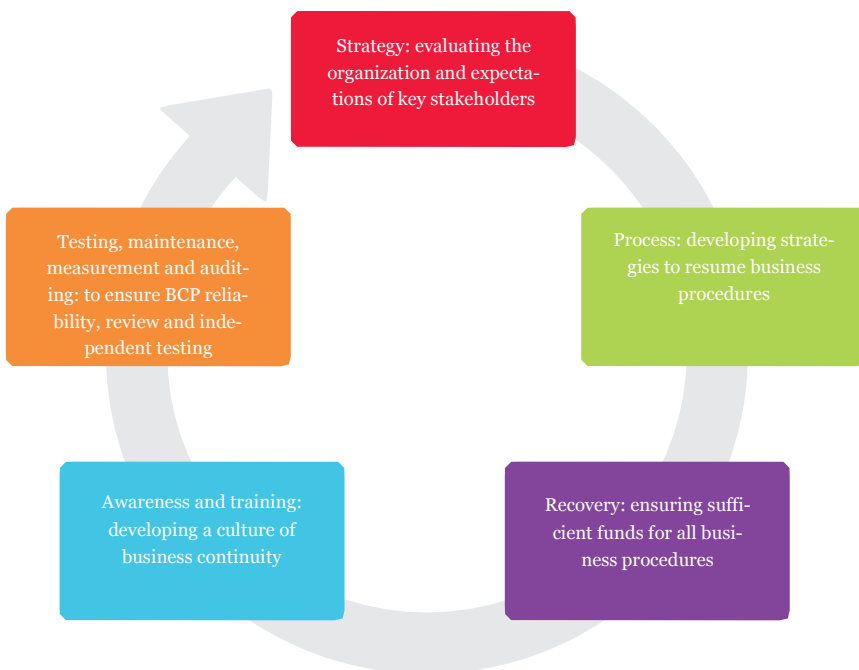
5.2.1. Proposed Membership

1. Coordinator – Risk Officer
2. Safety Officer (or whoever has that role)
3. Technology Director
4. Directors of Functional Departments and Business Units

5.2.2. Duties

1. To carry out the process of business continuity management and the BCP, which should contemplate the life-cycle phases of business continuity management

Figure 1



2. At least once a year, to direct the business impact review, an institutional risk assessment and monitoring of critical procedures and their vulnerability to major disruptions
3. To ensure that the BCP is updated to reflect changes in the institution's risk profile
4. To notify the Board of Directors and the Executive Directorate, on a regular basis, of the status and quality of business continuity management, emphasizing any gaps identified
5. To facilitate the procedural tests set out in the BCP

PHOTOS OF THE EARTHQUAKE OF APRIL 16, 2016



BEFORE

Portoviejo



AFTER

Portoviejo



BEFORE

Portoviejo



AFTER

Portoviejo



BEFORE

Portoviejo



AFTER

Portoviejo



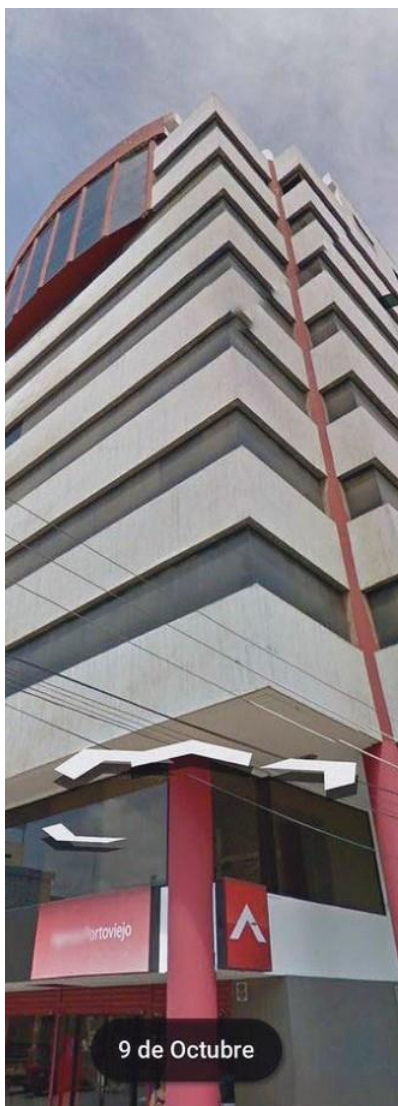
BEFORE

Portoviejo



AFTER

Portoviejo



BEFORE

Portoviejo



AFTER

Portoviejo



BEFORE

Portoviejo



AFTER

Portoviejo

Technical Guidebook

Post-Disaster Response and Recovery Plan for Develop- ment Finance Institutions

Response Manual
Ecuador 2016