USAID
FROM THE AMERICAN PEOPLE

USAID CLIMATE READY

KNOWLEDGE PRODUCTS

Business Continuity Planning Resources

October 2020

This document was produced for review by the United States Agency for international Development. It was prepared by DT Global for the USAID Climate Ready Project, Contract Number AID-492-H-17-00001.

USAID CLIMATE READY

KNOWLEDGE PRODUCTS

Business Continuity Planning Resources

Prepared by
DT Global

Cover Photo By
Arieta Sokota

Cover Photo Caption
Fishing boat approaching the town of London on Kiritimati Island in the Line Islands group of Kiribati.

Fiji Commerce & Employers Federation

FBDRC
Fiji Business Disaster Resilience Council

PIPSO
Pacific Islands Private Sector Organisation

USAID CLIMATE READY PROJECT

USAID Climate Ready is a five-year regional project funded by the USAID and implemented by DT Global, a United States based institutional contractor with worldwide experience implementing environment programs.

USAID Climate Ready works in 11 Pacific Island Countries (PICs): Federated States of Micronesia, Fiji, Kiribati, Palau, Papua New Guinea, Republic of the Marshall Islands, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

USAID Climate Ready works with PIC governments and other stakeholders to prioritize areas of support that align with their climate and disaster resilience plans and goals to:

1. Draft and implement policies that achieve national adaptation goals;
2. Access and utilize international sources of climate financing; and
3. Improve systems and expertise to better manage and monitor adaption projects.

USAID CLIMATE READY AND BUSINESS CONTINUITY PLANNING

In the Pacific region, the private sector is predominantly comprised of small and medium sized enterprises (SMEs) and about 70% of them operate in the agritourism-related sphere. These businesses are particularly vulnerable to the ever-present threat of climate change and natural disasters as they are generally lacking the resources to invest in disaster risk reduction and contingency planning.

The USAID Climate Ready Project teamed up with the Fiji Business Disaster Resilience Council, the Pacific Business Resilience Council and Chambers of Commerce from Fiji, Palau, Papua New Guinea, Republic of the Marshall Islands, Samoa and Vanuatu to empower small and medium businesses to better "disaster-proof" their operations through training and mentoring in the following material.

WELCOME

This publication is based on a two-day training of trainers workshop on Business Continuity Planning sponsored by the USAID Climate Ready Project in conjunction with Fiji Commerce and Employers' Federation (FCEF) and the Fiji Business Disaster Resilience Council (FBDRC).

The information herein has been drawn and adapted from a range of resources, especially materials developed by the Pacific Islands Private Sector Organisation (PIPSO), FBDRC, the Pacific Community and the Wellington Regional Emergency Management Office.

This collection of resources will build your awareness on:

- The concepts of disaster readiness and business continuity for business; and
- The key steps for a business to become disaster ready.

For additional details and information, follow the hyperlinks included throughout the document.

For more training tools and resources (including factsheets and videos in Bislama, English, Hindi, iTaukei, Marshallese, Pijin and Samoan languages, visit PIPSO - Business Disaster Support.

TRANSFORMING PRIVATE SECTOR ENGAGEMENT TO BUILD BUSINESS AND COMMUNITY RESILIENCE

"I'm told that 75% of companies without Business Continuity Plans fail within three years of a disaster. After Cyclone Winston, it was learnt that not many households and small businessess had insurance which also hindered their ability to bounce back."

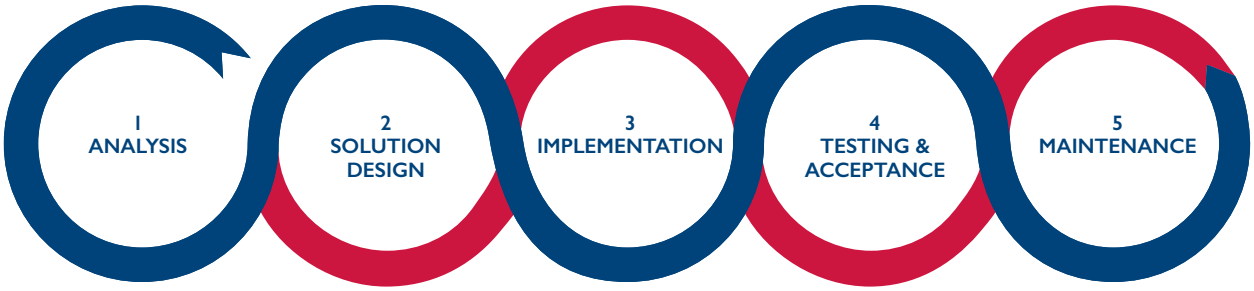
Patrick Suckling
Ambassador for the Environment,
Government of Australia

"Typically, businesses bear the brunt of the impacts of disaster events in the Pacific. 78% of the damage caused to Fiji by Tropical cyclone Winston in 2016 was accounted for by the private sector."

Cristelle Pratt
Deputy Secretary General of the
Pacific Islands Forum Secretariat

WHAT IS BUSINESS CONTINUITY PLANNING?

BUSINESS CONTINUITY PLANNING LIFECYCLE



1. ANALYSIS

Consists of impact analysis, threat analysis and impact scenarios.

BUSINESS IMPACT ANALYSIS (BIA)

A Business impact analysis (BIA) differentiates critical (urgent) and noncritical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

- Recovery Point Objective (RPO) - the acceptable latency of data that will not be recovered. For example, is it acceptable for the company to lose 2 days of data?

- Recovery Time Objective (RTO) - the acceptable amount of time to restore the function.

The RPO objective must ensure that the maximum tolerable data loss for each activity is not exceeded. The RTO objective must ensure that the Maximum Tolerable Period of Disruption for each activity is not exceeded.

BUSINESS IMPACT ANALYSIS (BIA)

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function.

THREAT AND RISK ANALYSIS

After defining recovery requirements, each potential threat may require unique recovery steps. The impact of an epidemic can be regarded as purely human and may be alleviated with technical and business solutions. However, if people behind these plans are affected by the disease, then the process can stumble.

COMMON THREATS INCLUDE:

- Epidemic;
- Earthquake;
- Fire;
- Flood;
- Cyber attack;
- Sabotage (insider or external threat);
- Hurricane or other major storm;
- Power outage;
- Water outage (supply interruption, contamination);
- Telecomms outage;
- IT outage;
- Terrorism/Piracy;
- War/civil disorder and
- Theft.

IMPACT SCENARIOS

After identifying the applicable threats, impact scenarios are considered to support the development of a business recovery plan.

Business continuity testing plans may document scenarios for each identified threats and impact scenarios. More localized impact scenarios – for example loss of a specific floor in a building – may also be documented.

The BC plans should reflect the requirements to recover the business in the widest possible damage. The risk assessment should cater to developing impact scenarios that are applicable to the business or the premises it operates. For example, it might not be logical to consider tsunami in the region of Mideast since the likelihood of such a threat is negligible.

RECOVERY REQUIREMENT

After the analysis phase, business and technical recovery requirements precede the solutions phase. Asset inventories allow for quick identification of deployable resources. For an office-based, IT-intensive business, the plan requirements may cover desks, human resources, applications, data, manual workarounds, computers and peripherals. Other business environments, such as production, distribution and warehousing will need to cover these elements, but likely have additional issues.

The robustness of an emergency management plan is dependent on how much money an organization or business can place into the plan. The organization must balance realistic feasibility with the need to properly prepare. In general, every $1 put into an emergency management plan will prevent $7 of loss.

2. SOLUTION DESIGN

Identifies the most cost-effective disaster recovery solution that meets two main requirements from the impact analysis stage.

For IT purposes, this is commonly expressed as the minimum application and data requirements and the time in which the minimum application and application data must be available.

Outside the IT domain, preservation of hard copy information, such as contracts, skilled staff or restoration of embedded technology in a process plant must be considered.

This phase overlaps with disaster recovery planning methodology. The solution phase determines:

- Crisis management command structure
- Secondary work sites
- Telecommunication architecture between primary and secondary work sites
- Data replication methodology between primary and secondary work sites
- Applications and data required at the secondary work site
- Physical data requirements at the secondary work site.

3. IMPLEMENTATION

Involves policy changes, material acquisitions, staffing and testing.

4. TESTING AND ORGANIZATIONAL ACCEPTANCE

The purpose of testing is to achieve organizational acceptance that the solution satisfies the recovery requirements. Plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws or solution implementation errors.
Testing may include:

- Crisis command team call-out testing
- Technical swing test from primary to secondary work locations
- Technical swing test from secondary to primary work locations
- Application test
- Business process test
- At minimum, testing is conducted on a biannual schedule.
- The 2008 book Exercising for Excellence, published by The British Standards Institution identified three types of exercises that can be employed when testing business continuity plans.

5. MAINTENANCE

Biannual or annual maintenance is broken down into three periodic activities. Issues found during the testing phase often must be reintroduced to the analysis phase.

A. INFORMATION/TARGETS

The BCP manual must evolve with the organization. Activating the call tree verifies the notification plan's efficiency as well as contact data accuracy. Like most business procedures, business continuity planning has its own jargon. Organisation-wide understanding of business continuity jargon is vital and glossaries are available. Types of organisational changes that should be identified and updated in the manual include:

- Staffing
- Important clients
- Vendors/suppliers
- Organization structure changes
- Company investment portfolio and mission statement
- Communication and transportation infrastructure such as roads and bridges

B. TECHNICAL

Specialized technical resources must be maintained. Checks include:

- Virus definition distribution
- Application security and service patch distribution
- Hardware operability
- Application operability
- Data verification
- Data application

C. TESTING AND VERIFICATION OF RECOVERY PROCEDURES

As work processes change, previous recovery procedures may no longer be suitable. Checks include:

- Are all work processes for critical functions documented?
- Have the systems used for critical functions changed?
- Are the documented work checklists meaningful and accurate?
- Do the documented work process recovery tasks and supporting disaster recovery infrastructure allow staff to recover within the predetermined recovery time objective?

WHAT IS DISASTER RECOVERY PLANNING?

Involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.

Disaster recovery focuses on the IT or technology systems supporting critical business functions, as opposed to business continuity which involves keeping all essential aspects of a business functioning despite significant disruptive events. Disaster recovery is therefore a subset of business continuity.

WHAT IS THE 12 STEP GUIDE TO DISASTER PROOFING YOUR BUSINESS TOOLKIT?

The 12 Step Guide to Disaster-Proofing Your Business Toolkit is a guide to help you better plan for and recovery from disasters.

It is comprised of videos, fact sheets, radio advertising scripts, text messages (SMS) and Facebook campaigns with guidelines and content ideas.

On the following pages, the 12 steps are outlined.

You can download the guide at pipso.org.fj/stayopen.

This 12 step guide and its content were developed by:

USAID
FROM THE AMERICAN PEOPLE

12 EASY STEPS TO DISASTER PROOF YOUR BUSINESS

DATE

FORM FILLED BY

BUSINESS NAME

STEP 1 - CORE PRODUCT/SERVICES

What products or services are fundemental to the survival of your business? (List 5)

STEP 2 - ESSENTIAL ROLES

What are the key roles needed to keep your business running?

Identify the tasks and the people capable of carrying out these key roles and write them into your business plan.
Quick Tip: Cross train members of your team to provide backup for different roles and skills.

STEP 3 - ESSENTIAL EQUIPMENT

What equipment is key to keep your business running?

If your equipment is damaged, what is your backup (if any)?

STEP 4 - ESSENTIAL SUPPLIES

What supplies are key to keep your business running?

If these supplies are disrupted, what is your backup?

STEP 5 - RELOCATION OPTIONS

If needed, do you have an alternative location for your business?

Identify some possible location options where you could relocate your business and who to contact in this case. Note any advantages and disadvantages.

STEP 6 - INSURANCE OPTIONS

Is your business insured? If not, what options are there?

Investigate local insurance options as some policies don't cover disaster such as cyclone or flash flooding so additional preparation will be required to protect your business and assets.

STEP 7 - DELEGATION OF AUTHORITY

Who has authority in times of disaster? If required is there a designated back-up?

Quick Tip: You might need some advice from a lawyer so that your trusted individuals are able to operate the business on your behalf during emergencies. Contact your local chamber of commerce or business councils for some free or discounted legal advice on this.

STEP 8 - EMERGENCY CONTACTS

List all key contacts, including employees, suppliers, insurance agents.

1. Name

   Contact | Designation

2. Name

   Contact | Designation

3. Name

   Contact | Designation

4. Name

   Contact | Designation

5. Name

   Contact | Designation

Insurance Company

Policy Number

Contact Person | Contact Number

Police | Fire | Ambulance

Any additional information you would like to include.

STEP 9 - BUSINESS RECORDS

How are your business records are stored? Are they backed up off site?

Quick Tip: Use off-site backups, such as online storage in the cloud, a portable hard drive that is taken home every day or kept in a fireproof safe. There are professional backup services available too, contact an IT provider for backup setups using NAS drives and other options.

STEP 10 - SAVE THIS PLAN

How will you save and share this plan?

Save this plan and ensure it can be accessed on laptops, tablets or mobile phones and easily at any time by you and your staff. Print some copies and have them available and accessible.

STEP 11 - DISASTER PREPAREDNESS

Are your staff trained in first aid? Who is your delegated first aid person?

Do you have an evacuation plan for a safe meeting point?

Do you have emergency supplies? i.e. first aid kit, water, tinned food, torch etc

Quick Tip: It is understandable that your staff's first priority in an emergency event is to check on their family members so encourage them to prepare their families for any disaster. This will ensure everyone's safety and will make it easier for your staff to return to work.

STEP 12 - PRACTICE & UPDATE THIS PLAN

Detail the schedule to run through and revise this plan.

Schedule regular dates to run through it step-by-step with your entire team and revise the plan yearly.

DATE FOR REVIEW	COMMENTS	COMPLETED

DATE FOR STAFF TRAINING	COMMENTS	COMPLETED

U.S. Agency for International Development

www.usaid.gov