



PIDC Secretariat

Business Continuity Plan

APRIL 2007

CONTENTS

1.0 Business Continuity Plan Overview

- 1.1 Introduction
- 1.2 Assumptions

2.0 Application of Business Continuity Plan

- 2.1 Structure of Plan
- 2.2 Roles and Responsibility
- 2.3 Assessment and Implementation

3.0 Continuous Improvement

- 3.1 Test and Maintain the Business Continuity Plan

PHASE ONE – NORMAL OPERATIONS

- 1.1 Maintain Effective, Ongoing Business Continuity Readiness
- 1.2 Maintain Secure Information Back Up Processes
- 1.3 Maintain Safe and Secure Facilities

PHASE TWO – EMERGENCY RESPONSE

- 2.1 Assess emergency status and risk and determine appropriate emergency response
- 2.2 Leadership & Staff Coordination
- 2.3 Close Office, Protect People & Assets (High Risk Option)
- 2.4 Evacuate Seconded Staff (High Risk Option)

PHASE THREE – BUSINESS CONTINUITY

- 3.1 Establish Alternative Office Site
- 3.2 Communicate With Stakeholders
- 3.3 Maintain Financial Management
- 3.4 Manage Information Systems
- 3.5 Protect Physical Assets & Equipment Security

PHASE FOUR – RESTORATION

- 4.1 Restore Business Operations, Assets, Staff Interests & Communications
- 4.2 Business Continuity Plan Improvements

APPENDIX A – KEY CONTACTS

APPENDIX B – ASSET REGISTER

APPENDIX C – RISK REGISTER

1.0 Overview of the Business Continuity Plan

1.1 Introduction

Every organisation can experience an emergency or disruption that may prevent it from continuing normal business operations and this can happen at any time. Such incidents can range from a natural disaster to a serious computer malfunction or unexpected political upheaval.

The purpose of the PIDC Business Continuity Plan (BCP) is to provide a clear set of operating instructions/procedures and outline contingencies in the event of an emergency or disruption to the normal operations of the PIDC Secretariat.

1.2 Assumptions

The BCP assumes that the political/security situation or circumstances unforeseen in Fiji prevent, substantially hinder, or disrupt the normal operation of the PIDC Secretariat.

The appropriate response to any emergency or disruption should be tailored to the situation as required and may include the implementation of the BCP in whole or in part.

The PIDC BCP has been developed to take into account the particular situation of the PIDC Secretariat, including location within the Forum Secretariat compound and the interests of the major donors: Australia, Fiji, New Zealand as well as the other PIDC members where directly affected. Where a situation arises requiring implementation of the BCP, the Secretariat will do so in consultation with these external agencies.

It is assumed that, where possible and practicable, the Secretariat will continue to function and provide service to the members of the PIDC.

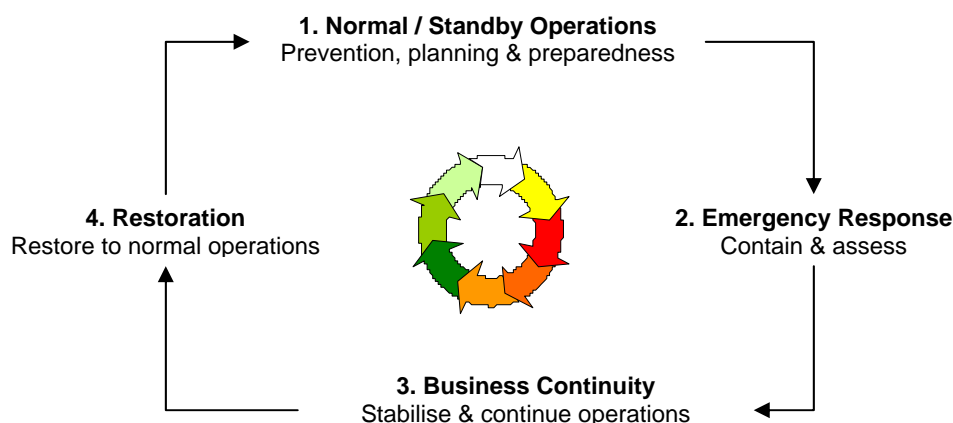
2.0 Application of the Business Continuity Plan

2.1 Structure of the Plan

The plan is structured into 4 phases. Each phase contains steps intended to return the Secretariat to normal operations after an emergency or disruption.

- (i) **Normal/Standby Operations.** These steps provide for the ongoing preventative control and ensures the continued readiness for unexpected events.
- (ii) **Emergency Response.** A check-list of actions/decisions to help assess impacts of an emergency or disruption.
- (iii) **Business Continuity.** Provides guidance to ensure the continuity of work and services.
- (iv) **Restoration.** Returning to normal operations.

Approach is in Four Phases



2.2 Roles and Responsibility

The Head of Secretariat (HoS) is the BCP Coordinator unless the HoS is out of the country in which case the PIDC Research Officer, in consultation with the Management Board, will be responsible for the implementation of the BCP.

The HoS will maintain the BCP and ensure that the Secretariat remains prepared for emergencies or disruptions. To ensure preparedness, the HoS will maintain a Risk Register and ensure that all staff, including officers seconded to the Secretariat, have a copy of the BCP and are aware of the emergency procedures.

The BCP Coordinator is responsible for:

BCP Plan Maintenance

Development of the BCP, testing & updating, maintaining the Risk Register, training, BCP documentation, availability of the BCP to staff and appropriate external stakeholders.

Evacuation & Closure

Approvals and clearances, communications, signage and directions, records destruction, office security, liaison with Management Board members, emergency kit, travel, accommodation.

Risk Assessment

Ongoing risk assessment, incident risk assessment, personnel impact assessments, disaster notifications, alternate office location.

People/HR resources

Health & safety, location, staff contact list, purchase and maintenance of a medical kit.

Communications

Notification reports, internal & external communications.

Information Systems

Back up information, secure storage, file management, telecommunications.

Finance & Assets

Interim cash and funds (in consultation with financial administrator), asset and systems registries.

Security

Security of alternate facilities, personnel safety & security contingencies.

2.3 Assessment and Implementation

Depending on the type of emergency or disruption, the Head of Secretariat, will implement the BCP after first making an assessment of the situation. Actions will be taken in consultation and coordination with Management Board members.

The table below provides a simple checklist of actions to be implemented and maintained under the 4 phases of the BCP.

Normal Operations Phase	<ul style="list-style-type: none">• Maintain effective, ongoing business continuity readiness• Maintain secure information back up processes• Maintain safe and secure facilities
Emergency Response Phase	<ul style="list-style-type: none">• Assess emergency status and risks• Determine and implement appropriate emergency responses• Leadership and staff coordination• Close office, protect people and assets (high risk option)• Evacuate seconded staff (high risk option)
Business Continuity Phase	<ul style="list-style-type: none">• Establish Alternative Office site• Communicate with stakeholders• Maintain financial management• Manage information systems• Protect physical assets and equipment security
Return to Normal Operations Phase	<ul style="list-style-type: none">• Restore business operations, assets, staff interests and communications• Business continuity plan improvements

3.0 Continuous Improvement

3.1 Test and maintain the BCP

The HoS will maintain the BCP and ensure that the Risk Register is updated and accounts for any new situation. The HoS will ensure that all staff and seconded

PIDC Business Continuity Plan

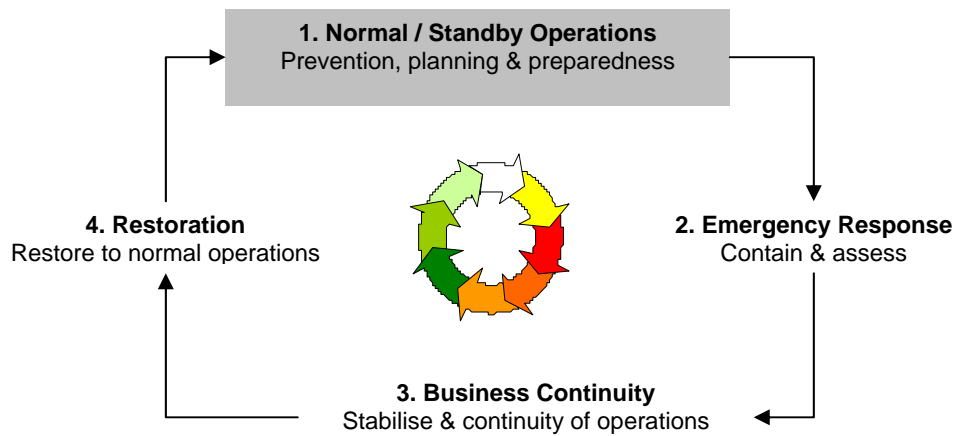
officers are aware of the BCP and have access to electronic and hard copies of the BCP. Copies of the BCP will also be made available to members of the PIDC Management Board.

The HoS will, in line with PIFS procedures, test the evacuation response and ensure staff, including seconded officers, are familiar with the PIFS evacuation procedures.

PHASE 1

NORMAL OPERATIONS

Approach is in Four Phases



PHASE 1 – NORMAL OPERATIONS

Prevention, planning & preparedness

1.1 Maintain Effective, Ongoing Business Continuity Readiness

Objective

To implement normal operating practices that minimise the impact of a localised disruption, to provide a foundation for an organised response and to ensure business continuity during the period of disruption.

TASK	DONE
Business Continuity Plan	
1. Develop and distribute a Business Continuity Plan.	
2. Establish individual responsibilities under the BCP and ensure staff are familiar with emergency evacuation procedures including, in accordance with PIFS, emergency drill.	
3. Maintain and update the BCP and make available copies at the Secretariat office, on the shared drive and distribute to Management Board members.	
Contact Lists	
4. Maintain and update emergency staff contact list and include the contact details of the appropriate Management Board members.	
Emergency Resources	
5. Maintain at least 4 weeks of key stationery.	
6. Maintain a fully stocked First-Aid kit and ensure all staff and seconded officers aware of the kits location.	

1.2 Maintain Secure Information Back Up Processes

Objective

To ensure that essential information is securely stored and backed-up for retrieval when required after an emergency or disruption.

TASK	DONE
Manage System Outages	
1. Systems outages to be reported to Corporate Services at PIFS and request assistance to provide alternate systems including telecommunications and electronic systems.	
2. Inform appropriate Management Board members of outage and need of assistance.	
Back Up Storage	
2. Ensure that all electronic information is regularly backed-up on independent storage system – CD/DVD	
3. Ensure copies of backed-up data stored in secure off-site location.	
Alternate System Capability	
4. Use office mobile phone in the event of a disruption to office telecommunications until an alternate system is available.	

PIDC Business Continuity Plan

5. Set up home PC if essential to establish alternate system.	
Paper-Based Information	
6. Lockable cabinets and cupboards for vital records or consider destruction if necessary	

1.3 Maintain Safe and Secure Facilities

Objective

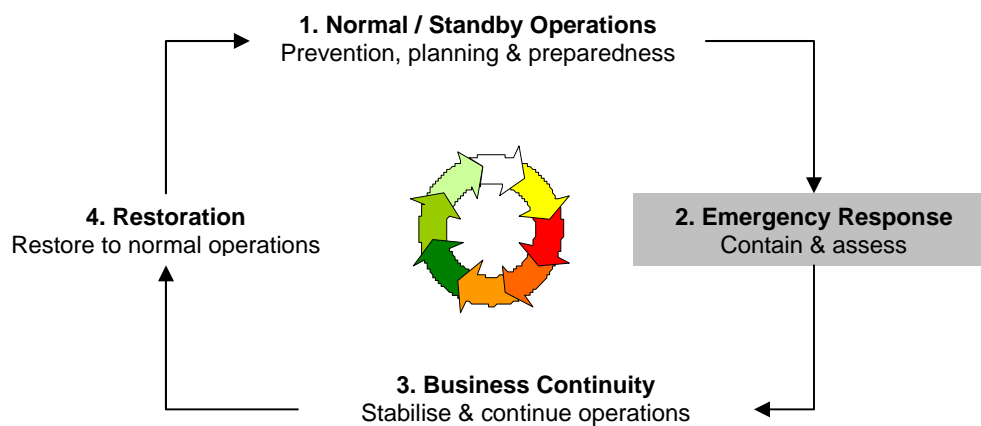
To protect and maintain property and ensuring that the staff working environment is safe and in accordance with the appropriate conditions.

TASK	DONE
Assets	
1. Maintain updated Asset Register.	
2. Copy of Asset Register to be held with the BCP at an off-site location.	
Building Facilities	
3. All staff aware of PIFS evacuation procedures in the event of an emergency.	
4. Maintain updated contact details for PIFS (Corporate Services) in the event of a problem with the office and/or facilities.	

PHASE 2

EMERGENCY RESPONSE

Approach is in Four Phases



PHASE 2 – EMERGENCY REPRONSE

Contain and Assess

2.1 Assess emergency status and risk and determine appropriate emergency response

Objective

To assess the damage or impact of an emergency or disruption at the Secretariat or within the operational environment outside of the Secretariat. To assist prioritising matters of safety and business operations following an emergency or disruption.

TASK	DONE
Immediate Response Assessment	
1. ascertain what has happened.	
2. Check on staff and, if appropriate, inform staff of the situation.	
3. If possible, contact the appropriate Management Board members to ascertain their situations and seek advice.	
4. Follow PIFS emergency procedures.	
5. If there is time and it is appropriate, take easily portable equipment from the office, such as mobile phone, HoS laptop, backup electronic files, etc.	
Business Impact Assessment	
6. Coordinate planning meeting involving staff and appropriate Management Board members. Involve PIFS if appropriate in terms of access and services.	
7. Ensure staff and appropriate Management Board members have copies of the BCP to retain throughout the disruption.	
8. Determine which services are down and which are still operational.	
9. Survey disruption to and assess impacts on: <ul style="list-style-type: none"> <input type="checkbox"/> Continuity of work in progress <input type="checkbox"/> Access to finance <input type="checkbox"/> Access and security of office information <input type="checkbox"/> Telecommunications <input type="checkbox"/> Facilities, assets, buildings and equipment <input type="checkbox"/> Update website where appropriate 	
10. Determine which staff are needed to maintain or build interim business continuity.	

2.2 Leadership & Staff Coordination

Objective

To ensure the process of implementation is carried out effectively and that the safety of staff and seconded officers is assured.

TASK	DONE
------	------

PIDC Business Continuity Plan

1. Note the physical location of all staff and ensure that staff can make contact with their families.	
2. Send home staff who are not required and to phone in or identify other means of contact for updates.	
3. Contact staff and notify them of work arrangements and timing.	
4. Arrange for staff transportation if public transport disrupted.	
5. Identify who is available for relocation to alternate office if the relocation option is necessary.	

2.3 Close Office, Protect People & Assets (High Risk Option)

Objective

To ensure the security of staff and vital records in the event of a high likelihood of unauthorised entry to office premises and risk to the safety of our personnel.

TASK	DONE
If the decision is made to close the Secretariat office the following procedures must be followed:	
1. Follow PIFS evacuation procedures	
2. Advise external contacts of evacuation	
3. Sign on door with emergency contact number (office cell phone).	
4. Staff to return home on advice from PIFS Emergency Coordinator and external contacts..	
5. Staff not to return to the Secretariat office until instructed by HoS.	
If it appears there may be a prolonged office closure:	
6. Assess security of electronic and paper data and consider the need for destruction – consult with external contacts and maintain awareness of PIFS recommendations.	
7. Leave sign on doors of absence and continuity or contact details for enquiries.	
8. Staff are not to attempt to return to work until told to by HoS or on advice from ANZ missions.	
Procedures if trapped at the office:	
9. Call family and friends to advise that you are safe but cannot leave work at the moment.	
10. Advise PIFS, if unaware, and external contacts.	
11. Locate emergency kit in office.	
12. As soon as it is safe, leave immediately and go directly home.	

2.4 Evacuate Seconded Staff (High Risk Option)

Objective

To evacuate seconded staff to a safe location and return the person to their country in the event of an imminent threat to personal safety.

TASK	DONE
-------------	-------------

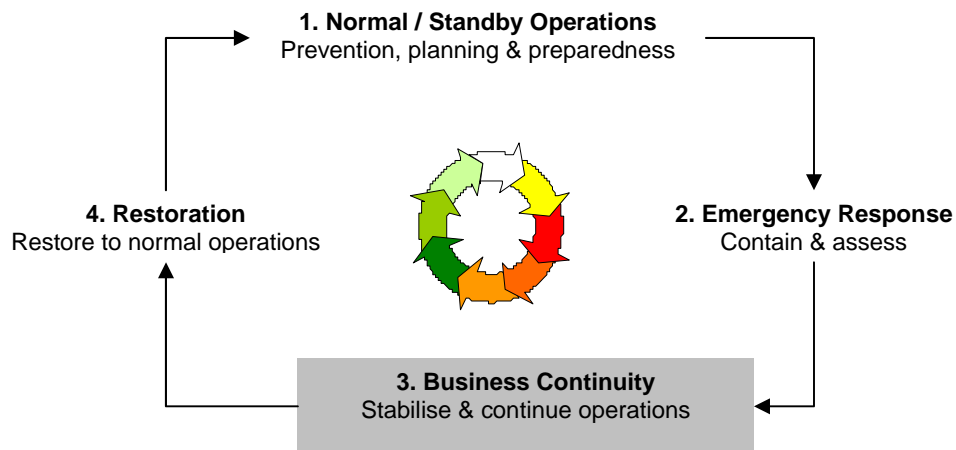
PIDC Business Continuity Plan

1. Discuss options with seconded staff and their home administration and ensure seconded officer's family are aware of the situation.	
2. Inform appropriate Management Board members of decision and request approval if additional expenditure necessary - unless threat is immediate prohibiting contact.	
3. Follow PIFS procedures and/or ascertain PIFS recommendations for its seconded staff.	
4. Ascertain safest and most direct escape route out of Suva or to a recognised safe location.	

PHASE 3

BUSINESS CONTINUITY

Approach is in Four Phases



PHASE 3 – BUSINESS CONTINUITY

Stabilise & Continue Operations

3.1 Establish Alternative Office Site

Objective

To establish an alternate office site from which to continue business operations.

TASK	DONE
Relocation Options	
1. Assess relocation options in light of seriousness and projected length of disruption <u>Option One</u> – remain in Fiji but relocate to recognised safe location (safe location to be determined in consultation with the High Commissions of Australian and New Zealand and in light of travel advisories for Fiji). Use Hotel or resort facilities or an apartment if the disruption is projected to last for a longer period. <u>Option Two</u> – Relocate outside of Fiji and establish office within the immigration department of one of the Management Board members.	
Equipment	
2. Equip work stations and establish telecommunications	
People	
3. Confirm which staff are required to maintain business continuity.	
4. Consider remote operations for staff not strictly required at alternate office site.	
5. Record and circulate all contact numbers.	
6. Orientate staff on interim processes and communication procedures.	
Property	
7. Consider security provision for staff and files at alternate office location.	
8. Alternate office site to be secure and safe with appropriate facilities should staff be required to leave their home in Suva	

3.2 Communicate With Stakeholders

Objective

To maintain communication with Staff and external stakeholders, particularly with the Management Board.

TASK	DONE
1. Maintain communication links with Secretariat staff keeping them updated on the situation and continuity of operations.	
2. Maintain communications with appropriate Management Board members.	

3.3 Maintain Financial Management

Objective

PIDC Business Continuity Plan

To ensure continuity of funds for ongoing business related expenses.

TASK	DONE
1. Liaise with financial administration provider for support including salaries and access to cash for accommodation and living expenses.	
2. Liaise with financial administration provider about longer term financial support options taking into account the situation.	
3. Maintain financial records for acquittal purposes.	

3.4 Manage Information Systems

Objective

To recover and establish key information systems critical to business continuity.

TASK	DONE
1. Maintain electronic files and records on disk including financial/expenditure records.	
2. Create a manual recording system for financial/expenditure.	
3. Maintain security of files and records.	

3.5 Protect Physical Assets & Equipment Security

Objective

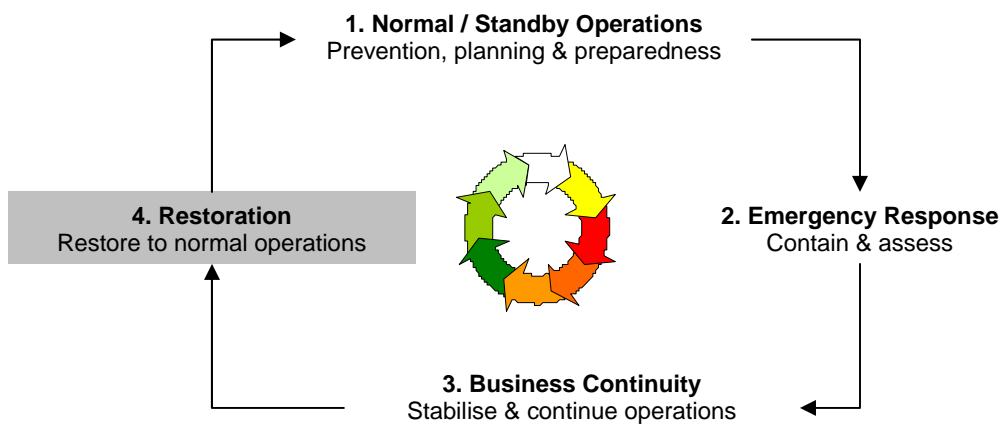
To ensure the security of alternate office premises and equipment.

TASK	DONE
1. If Secretariat office unusable, confirm with PIFS the security of equipment if unable to remove to alternate office site	
2. Ensure security of equipment at alternate office site.	

PHASE 4

RESTORATION

Approach is in Four Phases



PHASE 4 – RESTORATION

Return to normal operations

4.1 Restore Business Operations, Assets, Staff Interests & Communications

Objective

To take necessary steps to restore business operations to normal.

TASK	DONE
1. Liaise with PIFS and confirm return to Secretariat office.	
2. Inform staff of decision to return business operations to normal and confirm start dates.	
3. Maintain communications with appropriate Management Board members and then inform rest of PIDC membership.	
4. Update website.	
5. Check assets and property against the Asset Register.	

4.2 Business Continuity Plan Improvements

Objective

To debrief and share lessons learnt with staff, Management Board and the PIDC membership.

TASK	DONE
1. Debrief with Secretariat staff and discuss the performance of the BCP.	
2. Discuss outcomes with the Management Board.	
3. Identify gaps and lessons for remedial action.	
4. Update all Contact Lists and inventories	
5. Assign responsibility for remedial actions.	
6. Amend BCP where appropriate.	
7. Prepare BCP report for Management Board.	

APPENDIX A

Asset Register

The PIDC Secretariat Asset Register includes only the property of the Secretariat.

Last Updated: April 2007

Control #	Serial No.	Description	Model/Type	Supplier's Name	Purchase Price (local currency)	Acquisition Date	Physical Count (No.s)
1	CN OW4016 71618 5B2 CA59 CN OW4016 71618 57P B111 CN OW4016 71618 579 AAPC CN OFC237 71618 65C A835	Dell LCD Monitors		Graphic Equipment	See No. 7	Jan 2006	4
2		Notebook	IBM Thinkpad	<NZ based>	NZD\$2,200	2004	1
3	34817808592	Notebook	Dell	Graphic Equipment	FJD\$3,800	Jan 2006	1
4	PD01S	External CD drive	Dell	Graphic Equipment	See No. 3	Jan 2006	1
5	N/A	Docking Station	IBM	<NZ based>	NZD\$400	2004	1
6	N/A	Docking Station	Dell	Graphic Equipment	See No. 3	Jan 2006	1
7	DB PKG1S JN3GH1S	Hard drive tower	Dell	Graphic Equipment	FJD\$2,200 Inc monitor	Jan 2006	2
8	NZIS 25685	Laserjet printer	H/P 4300tn	<NZ based>	NZD\$ 1,000	2004	1
9	B1DY300060K	printer/scanner/fax/copier	Samsung	Graphic Equipment	FJD\$5,400	Jan 2006	1
10	N/A	Office desks	Office desks	Vinod Patel	FJD\$1,900	Jan 2006	4
11	N/A	Office Chairs	Office Chairs	Vinod Patel	FJD\$1,200	Jan 2006	4

APPENDIX B

Risk Register – Last updated April 2007

The Risk Register records details of key risks to the operation of the PIDC Secretariat. These risks may be specific to the Secretariats continued operation in Fiji or more general in their effect on the continuity of business regardless of location. Individual risks have been graded in terms of likelihood of occurring and seriousness of impact on the Secretariat. Initial plans for mitigating each of the high level risks, costs and responsibilities of the prescribed mitigation strategies and subsequent results.

Rating for LIKELIHOOD of Risk				Rating for SERIOUSNESS of Impact			
L	Rated as LOW	E	Rated as EXTREME	1	Rated as LOW	4	Rated as EXTREME
M	Rated as MEDIUM	N/A	NOT ASSESSED	2	Rated as MEDIUM	N/A	NOT ASSESSED
H	Rated as HIGH			3	Rated as HIGH		
Description of Risk	Likelihood	Seriousness	Mitigation Actions	Responsible Officer	Cost		
Ongoing political tensions within Fiji returning to December levels or higher.	M	4	Comprehensive Business Continuity Plan developed. Discussions with donors regarding options to move Secretariat if tensions return to earlier levels.	HoS in consultation with Donors and Management Board members.	Not available		
Resignation of staff or cessation of secondments to the Secretariat from PIDC member jurisdictions	M	3	Fill vacancies at earliest opportunity and request PIDC members to provide sufficient notice of cessation of secondments. Replace seconded officers from other member Jurisdictions or engage dedicated staff (F/T or P/T)	HoS, PIDC members and Management Board.	Not Available		
Inadequate funding to continue operations.	L	4	All PIDC members to share financial burden through member contributions to the operating costs.	PIDC members	Not Available		

PIDC Business Continuity Plan

Deterioration in relationship with Forum	L	2	Awareness of other location options within Suva or other PIDC member jurisdictions from which the Secretariat could operate.	HoS to maintain strong relationship with Forum, but inform Management Board of any change in relationship status	Not Available
Natural disaster such as tsunami or earthquake	L	3	Maintain awareness of the PIFS evacuation plan in the event of natural disaster and maintain contact with other offices in and around Suva	HoS, Secretariat Staff and PIDC Management Board members	Not Available