PremiumTrust Bank

BUSINESS CONTINUITY PLAN

Document Management Information

Document Title	**PremiumTrust Bank** - Business Continuity Plan
Document Ref. Number:	PTB/BCMS/PLN/0802
Issue Date	March 20, 2023
Document Author	Business Continuity Manager
Document Owner:	Chief Risk Officer
Version:	Version 1.0
Document Status:	Current

Role	Name	Designation
Author	Jeremiah Adesina	Business Continuity Manager
Reviewer/ Custodian	Kingsley Oriere	Chief Risk Officer
Owner	Kingsley Oriere	Chief Risk Officer

Distribution List

Name
All Staff

Reference Documents

Document Name	Document Number	Version No.
IT Disaster Recovery Plan		Version 1

Table of Contents

1.0 Introduction

PremiumTrust Bank recognises the importance of business survival and has developed this Business Continuity Plan (BCP) which outlines the policies and strategies to be implemented in the event of a disaster. The plan ensures an effective, organized response should an emergency disrupt normal office operating conditions for an immediate or indefinite period.

Without well-rehearsed contingency plans for disasters, PremiumTrust Bank employees have little option but to react in an uncoordinated manner in the event of a disaster. On the other hand, a Business Continuity team that has planned, practiced and fine-tuned options can align its actions to meet a problem of any magnitude. Regular drills enable personnel to act instinctively when disaster strikes.

2.0 Purpose and Scope

This document sets out a detailed plan to provide business continuity in the following situation:

1. A disruptive incident has occurred that significantly affects the Head Office of PremiumTrust Bank of Nigeria making them inaccessible to staff. This may be due to civil unrest/mob attack, flood, loss of power, physical damage or some other reasons.

2. The purpose of this plan is to recover the critical business processes at an alternative location and to provide staff access to them.

3. The procedures set out in this document should be used only as guidance when responding to an incident. The exact nature of an incident and its impact cannot be predicted with any degree of certainty and, so it is important that a good degree of common sense is used when deciding the actions to take.

However, it is intended that the plan set out here will prove useful in allowing the correct actions to be taken more quickly and based on information that is more accurate.

All members of staff named in this document will be given a copy which they must have available when required.

Contact details will be checked and updated at least two times a year. Changes to contact or other relevant details that occur outside of these scheduled checks should be sent to operationalrisk@premiumtrustbank.com as soon as possible after the change has occurred.

All personal information collected as part of the business continuity process and contained in this document will be used purely for the purposes of business continuity planning.

3.0 Objectives

The objectives of this business continuity plan are to:

- Ensure timely resumption of service to a level acceptable to the Bank’s customers and other Stakeholders.
- Provide a detailed description of how PremiumTrust Bank of Nigeria will respond to a disruptive incident affecting the critical business processes covered by this plan.
- Assign responsibilities with regards to incident response and the mode of BCP activation.
- Describe the facilities that are in place to help with the implementation of the plan.
- Define how decisions will be taken regarding our response to an incident.
- Explain how communication within the organisation and with external parties will be handled.
- Provide contact details for key people and external agencies and suppliers.
- Define what will happen once the incident is resolved, and the business continuity teams have addressed the incident.

This BCP also seeks to minimise:

- The impact to PremiumTrust Bank’s public image and adverse financial effects of a disruption.
- The number and frequency of 'ad hoc' decisions which must be made immediately after an incident in the absence of a pre-defined procedure.
- Inconvenience and potential disruption to other business functions.
- The need to develop and implement new procedures once the disruption has occurred.
- The loss of data and information, recognising that some loss is inevitable.
- Confusion and exposure to errors, omissions, and unnecessary duplication of effort and
- The time it takes to execute response, recovery, and resumption processes.

4.0 Assumption

This plan is based on the following assumption:

- IT services will be provided to the alternate locations from the Data Centre (DC) at MainOne Ogombo, Victoria Island.

- The business processes covered by this plan are those with Recovery Time Objectives (RTOs) that are less than 6 hours.

5.0 Activation Criteria and Procedures

This plan may be activated in two main scenarios:

1. In response to a major disruptive incident that has resulted in the organisation's Incident Response Procedure being activated.

2. As a recovery for a smaller, more localised event, which although not serious enough to result in activation of the Incident Response Procedure, requires action to address its impact.

5.1 As Part of the Incident Response Procedure

Notice will be received from the Incident Response Team (IRT) by telephone to the main plan owner (or deputy) if this plan is required to be activated. This will depend upon the incident that has occurred and the scope of its effects.

It is likely that this plan will be one of several that will be activated and co-ordination across the various plans will be needed.

5.2 Localized Activation

It will be up to the main plan owner (or deputy) to request of top management that the plan be activated and to inform them once this has been done.

5.3 Activation Procedure

Once the decision has been taken to activate the plan, the plan owner (or deputy) will contact the members of the recovery team using the contact details at Appendix A. They will then be informed of the nature of the incident and asked to assemble at the primary location specified below.

PremiumTrust Bank Head Office,
Plot 1612 Adeola Hopewell, Victoria Island, Lagos, Nigeria

If the primary location is unavailable, the plan owner will request that the team assemble at the alternative location specified below:

PremiumTrust Bank RCCG Branch,
Km 46 Lagos Ibadan Expressway,
Redemption Camp, Mowe
Ogun State, Nigeria

An initial briefing will then be held at which the plan owner will:

- Explain why the plan has been activated.
- Describe the impact of the incident.
- Outline what needs to be achieved by the team.
- Allocate tasks according to the checklists detailed in the plan.
- Address any questions the team may have.
- Set out the method and frequency of communication within the team.

The staff in the affected location will assemble at the muster points within the premises of the location specified below once this plan has been activated.

PremiumTrust Bank, Executive Car Park Space
Plot 1612, Adeola Hopewell, Victoria Island, Lagos

5.4 Critical Business Units and their Alternate Locations

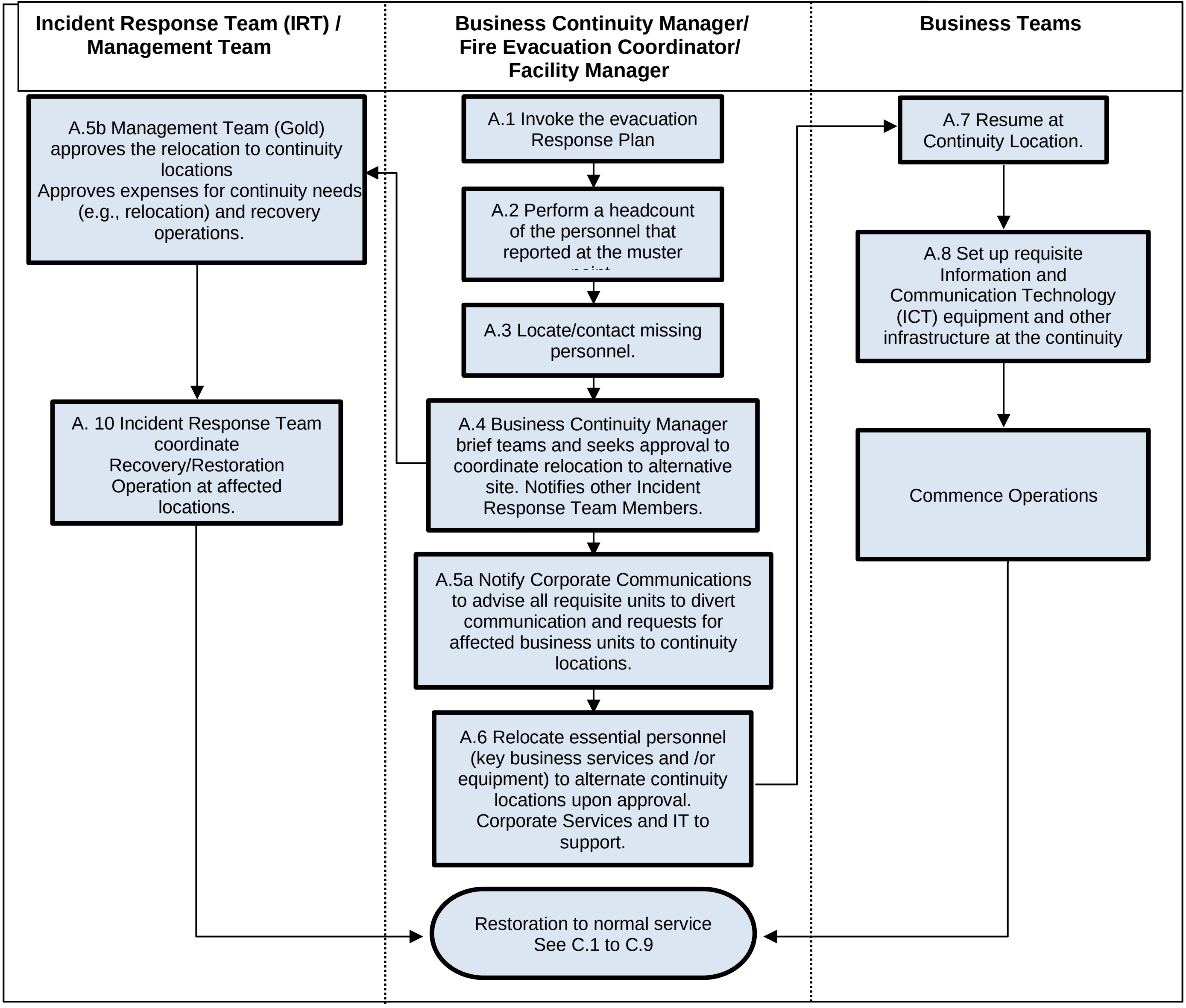
SN	Department	Alternate Work Area
1	Branch Services	Designated Business Hub
2	Central Operations	Designated Business Hub
3	Conduct & Compliance	Work from Home
4	Corporate Communications	Work from Home
5	Corporate Services	Work from Home
6	Customer Experience	Designated Business Hub
7	Digital Banking	Designated Business Hub
8	E-Business	Designated Business Hub
9	Finance	Work from Home
10	Information Security	Work from Home
11	Information Security	Work from Home
12	Information Security	Work from Home
13	Information Technology	Designated Business Hub
14	Internal Audit	Work from Home
15	Legal & Company Secretariat	Work from Home
16	People Management Group	Work from Home
17	Project Management Office	Designated Business Hub
18	Propositions	Work from Home
19	Risk Management	Work from Home
20	Strategy & Innovation	Work from Home
21	Treasury	Designated Business Hub

6.0 Implementation Procedure

6.1 Overview

The response activities are as shown in the workflow below. The checklists in Appendices E, F and G should be used in conjunction with the more detailed procedures in the workflow.

Scenario: Evacuation of personnel from the Head Office to an alternative location as a result of a major disruptive incidents such as flood civil unrest, protests, fire or a temporary loss of access to the Head Office buildingA


Incident Response Team (IRT) / Management Team
Business Continuity Manager/ Fire Evacuation Coordinator/ Facility Manager
Business Teams
A.5b Management Team (Gold) approves the relocation to continuity locations Approves expenses for continuity needs (e.g., relocation) and recovery operations.
A. 10 Incident Response Team coordinate Recovery/Restoration Operation at affected locations.
A.1 Invoke the evacuation Response Plan
A.2 Perform a headcount of the personnel that reported at the muster
A.3 Locate/contact missing personnel.
A.4 Business Continuity Manager brief teams and seeks approval to coordinate relocation to alternative site. Notifies other Incident Response Team Members.
A.5a Notify Corporate Communications to advise all requisite units to divert communication and requests for affected business units to continuity locations.
A.6 Relocate essential personnel (key business services and /or equipment) to alternate continuity locations upon approval. Corporate Services and IT to support.
Restoration to normal service See C.1 to C.9
A.7 Resume at Continuity Location.
A.8 Set up requisite Information and Communication Technology (ICT) equipment and other infrastructure at the continuity
Commence Operations

6.2 Recovery Checklists

The following checklists should be used in conjunction with the more detailed procedures listed as appendices to this document.

6.3 Business Team Recovery Checklists

Task	Procedure reference	Target Completion Date/Time	Actual Completion Date/Time	Signature
Confirm with Incident Response Team the likely elapsed time before an interim service will be available				
Communicate with Business Teams to set expectations				
Divert phones according to procedure at Appendix				
Allocate manual tasks to appropriate teams				
Identify key users and ask them to go to the alternative site once the IT Recovery Team has recovered sufficient IT systems				
Test systems once go-ahead given by IT Recovery Team				

7.0 Roles, Responsibilities and Authorities

7.1 Continuity Teams

The Continuity Teams and Personnel consists of the following:

Name	Title	Role In Plan	Contact Number
Management Team (Gold)	Management Team	**Top Management** ▸ Approve the relocation to the continuity location.	See Incident Response Plan
Incident Response Team (Silver)	Incident Response Team	**Incident Response Team** ▸ Acts as interface with the executive management and other high-level stakeholders to invoke a response.	Appendix A – Plan Activation Contact Sheet
Emergency Response Team (Fire Marshalls, Security team and Health & Safety Officer)	Evacuation Administrators and Fire Wardens	**Evacuation Administrator/Co-ordinator/Incident Liaison** ▸ Ensure overall success of the evacuation process. ▸ Ensure that all personnel are evacuated within their physical area. ▸ Assesses the extent and impact of the incident. ▸ Provides first-person account of the situation to the IRT and provide updates on an on-going basis required for decision-making by the IRT	Appendix D – Internal Contact Telephone Numbers
Damage Assessment/ Salvage Team	Premises Managers, Facility Management	**Damage Assessment for Incident Site** ▸ Assess the extent of damage caused by the incident. ▸ Identify what can be salvaged and reused if necessary. ▸ Provide an update on when the affected site will be available following an incident for recovery	Appendix D – Internal Contact Telephone Numbers
Communications Team	Communications Team	**Communication (Internal and External)** ▸ Decides the level, frequency and content of communications with	Appendix D – Internal Contact Telephone Numbers

		external parties such as the media. - Responsible for ensuring internal and external communications are effective. - Defines approach to keeping affected parties informed e.g., customers, shareholders.	

7.2 Business Recovery Team

The members of the Business Recovery Team will depend upon the locations affected and may include:

Name	Title	Role in Plan
Business Units Team Leads/Group Heads See Business Impact Analysis (BIA) Workbook	Business Units Team Leads/Group Heads Liaison	• Continuity of Business Team operation • Managing the establishment of key business services at continuity locations. • Managing the establishment of manual business procedures until such time when primary locations are recovered.
Business Units Internal Dependencies See Business Impact Analysis (BIA) Workbook	Business Units Liaison	• Provision of service to affected units or group activities whose output is required to perform this service

8.0 Communication Requirements and Procedures

All requests for information from the media or other sources should be referred to the Head, Brands & Corporate Communications.

8.1 Communications Procedures

It is vital that effective communications are maintained between all parties involved in the incident response.

8.2 Means of Communication

The primary means of communication during an incident will be telephone, both landline and mobile. In the event of telephone communications, being unavailable provision may be made for the use of radio communications, although the usable range of such equipment should be assessed.

Email should not be used unless telephone and equivalent alternatives are unavailable.

8.3 Communication Guidelines

The following guidelines should be followed in all communications:

- Be calm and avoid lengthy conversation.
- Internal team members should refer information requests to the Incident Response Team
- If the call is answered by someone other than the contact:
  - Ask if the contact is available elsewhere.
  - If they cannot be contacted leave a message to contact, you on a given number.
  - Do not provide details of the Incident.
- Always document call time details, responses and actions.

All communications should be clearly and accurately recorded using the form at Appendix C to this document.

8.3.1 External Communication

Depending on the incident, there may be a variety of external parties that will be communicated with during the response. It is important that the information released to third parties is managed so that it is timely and accurate.

Calls that are not from agencies directly involved in the incident response (such as the media) should be referred to the Head, Brands & Corporate Communications.

Emergency responders such as the police, fire and ambulance services will be well-trained in incident handling and will have their own structured methods for communication and every effort should be made to comply with these. A listing of the phonetic alphabet used by the emergency services is at Appendix I.

8.3.2 Communication with the Media

In general, the communication strategy with respect to the media will be to issue regular updates via top management.

No members of staff should give an interview with the media.

9.0 Internal and External Interdependencies and Interactions

This business continuity plan is part of a set of plans that has been created to address a variety of potential situations affecting PremiumTrust Bank of Nigeria.

Depending on the nature and scope of the incident that has occurred, it may be necessary to co-ordinate the execution of this plan with that of others.

The key business continuity plans that may have an interdependency with this plan are as follows:

Document reference	Plan title	Plan Description	Plan Owner
Plan01	IT Disaster Recovery Plan	Failover of IT systems to Disaster Recovery Site	GH, Information Technology
Plan02	Emergency Response Plan	Response to fire or other internal emergency	Chief Risk Officer
Plan03	Communications Plan	Communication during an incident	Head, Brands & Corporate Communications
Plan04	Departmental Business Continuity Plan	Loss of physical access to Head Office, location with critical department specific information	Heads of critical departments
Plan05	Incident Response Procedure	Response procedure to emergency incidents	Chief Risk Officer

Contact details for the above plan owners can be found at Appendix D. If the Incident Response Procedure has been activated, communication should initially be channelled through the IRT.

This plan also depends upon the following external interactions:

External Agency	Dependency	Comments
National Emergency Management Agency	Emergency Response	Emergency: 0800CALLNEMA, 080022556362
Federal Fire Service	Emergency Response	Emergency: 08032003557 099 for Fire Outbreak. 098 for Flood 097 for Collapsed Building
Lagos State Fire Service	Emergency Response	Lagos Emergency Toll Free Lines: 767 or 112 Onikan Fire Station: 08186404240
Nigeria Police Force	Emergency Response	08036634061

10.0 Resource Requirements

The resources required to implement this business continuity plan are as follows:

Resource	Quantity	Source	Comments
Desktop PCs	Based on number of business unit's personnel without laptops	Information Technology (IT)	See Business Impact Analysis Workbook
Office space with desks and chairs	Based on number of business unit's personnel without laptops	Corporate Services	See Business Impact Analysis Workbook

These resources will need to be made available in order for the plan to be completed in a timely fashion. Requests for further resources (or issues with the identified resources) should be escalated to the Incident Response Team (if the Incident Response Procedure has been activated) or via normal management channels.

11.0 Information Flow and Documentation Processes

During an incident response, it is vital that information flows effectively around the response teams and that certain processes are followed to ensure that actions and messages are recorded correctly.

If the Incident Response Procedure has been activated, then regular updates on the situation should be given to the Incident Response Team (IRT). The IRT Team Leader will specify the frequency of these updates, although significant events would be communicated immediately.

Within the local recovery teams for this business continuity plan, the plan owner will decide how often progress updates should be given and is responsible for co-ordination between the IT Recovery and Business Recovery teams.

Actions that are decided upon as a result of progress meetings should be recorded using the template form at Appendix B.

12.0 Restoration of Normal Service

Once this plan has been implemented and the servers recovered at the alternate location, a decision will need to be made about how long this situation will be required.

This will depend upon several factors including the extent of the damage to the primary site and how long it takes before the infrastructure required to house the servers is back in place.

Top management should decide when a restoration of normal service should be attempted based on advice from all involved parties. It is likely that this will be done over a period of low business activity e.g. a weekend or public holiday.

The checklist in 12.1.3 should be used to move the services back to their original location (or permanent replacement location). This checklist assumes that the required hardware and network connectivity has been replaced and is operational at the primary site before work begins.

12.1 Continuity Checklists

12.1.1 Incident Response Team (Evacuation) Checklist

Step	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
	Scenario: Evacuation of personnel from Head Office as a result of a major disruptive incidents e.g., flood, riots, protests, fire or a temporary loss of access to the Head Office.				
A1	Invoke the Evacuation Response Plan.	Business Continuity Manager			
A2	Perform a head count of personnel that reported to the muster point	Chief Security Officer			
A3	Locate/contact missing personnel.	GH, Corporate Services			
A4	Business Continuity Manager briefs team and seeks approval to co-ordinate relocation to continuity location. Notify other Incident Response Team members	Business Continuity Manager			
A5a	Notify Corporate Communication to advise all requisite units to divert communication and requests for affected business units to continuity locations.	Business Continuity Manager			
A5b	Management Team approves the relocation to continuity locations. Approves expenses for continuity needs (e.g. relocation) and recovery operation	Executive Management			
A6	Relocate essential personnel (key business services and/or equipment) to alternate continuity locations upon approval. General Internal Service and IT to support.	Business Continuity Manager			
A7	Resume at continuity location	Critical Business Functions			

Step	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
	Scenario: Evacuation of personnel from Head Office as a result of a major disruptive incidents e.g., flood, riots, protests, fire or a temporary loss of access to the Head Office.				
A8	Set-up requisite Information and Communication Technology (ICT) equipment and other infrastructure at the continuity locations (if required).	GH, ITG			
A9	Commence operations	Critical Business Functions			
A10	Incident Response Team Coordinates Recovery/Restoration Operation at affected locations.	Business Continuity Manager			
A11	Restoration to normal service. See Checklist below C.1 to C.7	Critical Business Functions			

12.1.2 Business Team Response Checklist

	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
B1	Confirm with Incident Response Team the likely elapsed time before an interim service will be available.	Business Continuity Manager			
B2	Communicate with other members of the Business Team to set expectations.	HODs of critical functions			
B3	Allocate manual tasks to appropriate teams.	HODs of critical functions			
B4	Identify key users and relocate them to alternative continuity locations once IRT advises continuity locations.	Business Continuity Manager			

	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
B5	Commence operation of critical services at continuity locations	HODs of critical functions			

12.1.3 *Restoration/Recovery (Salvage Team) Checklist*

	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
C1	Upon the completion of damage and impact assessment to personnel, site and equipment. Ensure that the safety and status of personnel have been assured, and emergency conditions at the primary location have abated.	Business Continuity Manager			
C2	Initiate restoration/recovery operations. As a starting point, initiate the restoration of key business activities requirements at the primary location.	HODs of critical functions			
C3	Upon the completion of restoration/recovery operation of the facilities and equipment (if damaged) at the primary location, Contact the Facilities Managers of the primary location and Head of business units to make provision for the relocation of personnel (key business activities) to restored primary location.	Business Continuity Manager			
C4	Relocation of personnel to restored primary location.	Business Continuity Manager			
C5	Check that the provided Information and Communication Technology (ICT) equipment are correct and complete (if any)	GH, ITG			
C5	Initiate the restoration to normal service.	Business Continuity Manager & HODs of critical functions.			

	Task	Responsibility	Target Completion Date/Time	Actual Completion Date/Time	Signature
C6	Business Teams commence operations.	HODs of critical functions.			
C7	Divert communication back to primary location.	Business Continuity Manager			

13.0 BUSINESS CONTINUITY STRATEGY

The purpose of the business continuity strategy is to assess alternatives and define the strategies that will be used to deliver the degree of business continuity that has been identified as being needed. These strategies are then formulated into more detailed business continuity procedures which set out what actions will be taken before, during and after identified risks to continuity of the business.
Below are the business continuity strategies that are obtainable within PremiumTrust bank.

13.1 Business Continuity Risk/Threats & Available Strategies

Risk	Available Strategies
People Unavailability	1. Succession Planning: HR ensures that key personnel within the Bank are identified, and backup is identified and assigned to learn. 2. Cross departmental training: At on-boarding new personnel are encouraged to learn other department processes to serve as backup to the department when personnel are not available. 3. Interdepartmental knowledge sharing sessions
IT Failure	1. Third Party Management: SLAs with vendors included service level agreements and chargebacks were also introduced for downtime above agreed. 2. DR Site: The Bank established DR site for critical applications; daily/weekly back-up of severs. 3. IT help desk portal to manage and resolve system disruptions 4. Alternate/Secondary ISP 5. Stop gap laptops available in case of laptop failure 6. Realtime replication of the Bank’s core application at the Bank’s DR site
Building Unavailability	1. Staff can work from the nearest branch 2. Work from home strategy is also adopted
Loss of Power	1. Availability of primary generator and back-up generator, UPS, Inverters etc. 2. Proper maintenance of the Bank’s generator, UPS, inventors etc.

	3. Availability of nearest branch site in the event of relocation etc.
Pandemic/ Epidemic	1. Staff can work remotely and from the nearest branch closest to them 2. Remote working policy development and review 3. Robust HMO plan to cover remote hospital services 4. Regular staff sensitization on precautions 5. Regular review of guidance

13.2 Business Continuity Strategies Before, During & After a Disruption and Resources Requirements

Risk Event Type	Before	During	After	Resources Requirement
Natural Disaster i.e., Flood, Fire	1. Ensure insurance coverage on buildings belonging to the organization. 2. Install smoke alarms on every floor and test the alarm. 3. Ensure effective drainage system 4. Perform drills and natural disaster response awareness 5. Ensure fire extinguishers are functioning 6. Create a disaster preparedness plan for the property ahead of time	1. Alarm is activated, and evacuation performed 2. Firefighting using extinguishers and fire hose 3. Engaging Fire Service	1. Check your insurance coverage. 2. Assess the damage and compile repair bids 3. Repair and replace properties affected by the fire Check and replace Firefighting equipment	• Fire/smoke alarm systems • Fire extinguishers • Fire hose
Unavailability of personnel or lack of trained personnel	1. Succession planning 2. Job rotation 3. Knowledge management and retention 4. Create a training plan 5. Plan leave to ensure 2 key staff are not unavailable at the same time.	1. Outsourcing	1. Review training plan	• Budget for Training • Employing successor for key roles within the Bank
Cyber Attack i.e., Data corruption, Unauthorized access to data,	1. Employ a DAM /Data loss prevention tools 2. Training and awareness on cyber-attack responses	1. Communicate the breach with their employees and	1. Patch management 2. Outsource security operations	• Cyber security tools

Loss of data, Ransomware	3. Encrypt and back up data 4. Use robust anti-malware and firewall software 5. Ensure Endpoint Protection 6. Access control and management 7. Password control and management 8. Deploy a SIEM tool for monitoring	implement security awareness training. 2. Implement crisis management plan 3. Mobilize response team 4. Restore backup	3. Check/review security plans 4. Conduct investigations for root cause	
Third party risks i.e., unavailability of vendor services/ personnel, lack of vendor support	1. SLA with third party 2. Third party performance evaluation 3. Utilize secure remote access tools 4. Create a database of existing third party 5. Perform due diligence on third pa	1. Communicate with third party 2. Alternative/Substitute third party 3. Restrict access for cases of breaches	1. Blacklist unavailable third party (Review third party list) 2. Review third party risk/ perform risk assessment for existing third party 3. Establish an incidence response team	• Establish Back up and redundant vendors
Technology/ IT Services failure i.e., application/ technology failure, laptop failure, ATM failure, Access control door failure,	1.Establishment of incident response team 2. Establishment of Disaster Recovery Site 3. Replication of critical systems and applications in DR site	1.Activation of Disaster recovery plan 2. Failover to DR for critical systems and applications 3. Communication to employees on incidence 4. Provision of additional connectivity service to key roles 5. Provision of laptops for staff with faulty systems	1. Communication on restoration of normal services 2. Restoring IT services to secondary location	• DR Site • Storage for replication at the DR site • Extra workstation
Civil issues/ unrest i.e., protests, riot, strike actions, litigation	1. Creation of Business Continuity Plans 2. Provision of remote working resources	1. Activation of Business Continuity Plan 2. Employees revert to working from home or nearest branch.	1. Communication on restoration of normal services 2. Return to normal working conditions	• Laptops for critical staff using desktop in the office

	3. VPN provisioning for access to core applications	3. Provision of Mobile Data for employees		- VPN access for staff that require VPN - Internet data budget for employees
Loss of Power i.e., total grid collapse, generator failure, UPS failure	1. Provision of backup generators 2. Follow routine servicing of generating sets 3. Establish contact with suppliers of Diesel/Petrol	1. Power up of the power generating sets 2. Get in touch with power distribution company (EKEDC)	1. Ensure routine servicing of generating sets	- Backup generator - UPS - Diesel/ Petrol
Pandemic/ Epidemic i.e., COVID 19, SARS, EBOOLA	1. VPN provisioning for access to core applications 2. Remote access provisioning 3. Provision of remote working resources	1. Activation of Business Continuity Plan 2. Employees revert to working from home 3. Provision of Data for employees	1. Gradual return to normal working conditions 2. Ensure social distancing within the office on return to the office 3. Ensure all safety protocols are observed and sick employees are disallowed from the office	- Mobile workstation - Internet data - VPN access

13.3 Business Continuity Strategies by RTOs

S/N	Activities	Disruption Scenario	Recovery Time Objective (RTO)	Strategy	Resources required
1	All critical activities as stated in the BIA summary report	Cyber Attack i.e., Data corruption, Unauthorized access to data, Loss of data, Ransomware	<=1 hour	- Failover to the DR site (hot site) - Communicate the breach to stakeholders	Disaster Recovery Management team - Network - Physical/Virtual servers - VPN - Cyber security tools
			<=4 hours	- Failover to the DR site - Communicate the breach to stakeholders	
			<=12 hours	- Failover using back-up tapes - Communicate the breach to stakeholders	
			<=24 hours	- Failover using back-up tapes	

				• Communicate the breach to stakeholders	
2	All critical activities as stated in the BIA summary report	Unavailability of personnel or lack of trained personnel	<=1 hour	• Deploy personnel in other departments to perform the tasks in the interim • Identify back-up staff for all key roles • Recall employees on leave (where applicable) • Activate succession plan for key roles (management roles)	• People • Budget for training • Performing job rotation
			<=4 hours	• Deploy personnel in other departments to perform the tasks in the interim. • Recall employees on leave (leave applicable) • Identify back-up staff for all key roles	
			<=12 hours	• Recall employees on leave (where applicable) • Deploy personnel in other departments to perform the tasks in the interim	
			<=24 hours	• Recall employees on leave (where applicable) • Employee redeployment to other department	
3	All critical activities as stated in the BIA summary report	Technology/IT Services failure i.e., application/technology failure, laptop failure, Access control door failure	<=1 hour	• Failover to the DR site • Communicate the incident/downtime to stakeholders. • Provision of additional connectivity service to key roles • Provision of laptop for staff with faulty systems • In extreme cases, activation of the DRP	• Storage for the replication at the DR site • Extra workstation • Physical/virtual servers • VPN
			<=4 hours	• Failover to the DR site • Communicate the incident/downtime to stakeholders. • Provision of additional connectivity service to key roles • Provision of laptop for staff with faulty systems • In extreme cases, activation of the DRP	
			<=12 hours	• Failover to the DR site • Communicate the incident/downtime to stakeholders • Provision of additional connectivity service to key roles • Provision of laptop for staff with faulty systems	
			<=24 hours	• Troubleshoot the problem	

				• Failover using back-up tapes • Communicate the incident/downtime to stakeholders • Switch to alternate vendor/service provider (e.g., DR VPN, alternate ISP etc) • Provision of laptops for staff with faulty systems	
4	All critical activities as stated in the BIA summary report	Civil issues/ unrest i.e., protests riot, strike actions, litigation	<=1 hour	• Provision of hotel accommodation and security for critical staff (where necessary) • Activation of Business Continuity Plan • Employees revert to working from home or nearest branch • Provision of mobile data for employees • Provision of VPN for employees	• Laptops for staff • VPN access for staff • Internet data budget for employees • Alternate office location
			<=4 hours	• Activation of Business Continuity Plan • Employees revert to working from home or nearest branch • Provision of mobile data for employees • Provision of VPN for employees	
			<=12 hours <=24 hours	• Activation of Business Continuity Plan • Employees revert to working from home or nearest branch • Provision of mobile data for employees • Provision of VPN for employees	
5	All critical activities as stated in the BIA summary report	Third party risks i.e., unavailability of vendor services/personnel, lack of vendor support	<=1 hour <=4 hours	• Communicate with third party • Engage Alternate/Substitute third party • Restrict access for cases of breaches	• Identify alternate providers for critical services
			<=12 hours <=24 hours	• Troubleshoot the issue/internal resolution techniques • Communicate with third party • Engage Alternate/Substitute third party • Restrict access for cases of breaches	
6	All critical activities as stated in the	Fire	<=1 hour <=4 hours	• Alarm is activated and evacuation performed • Firefighting using extinguishers and fire hose • Engaging fire service	• Fire/Smoke alarm systems • Fire extinguishers

	BIA summary report			• Staff are advised to work from nearest branch or work from home	• Fire hose • Fire personnel
			<=12 hours <=24 hours	• Alarm is activated and evacuation performed • Firefighting using extinguishers and fire hose • Engaging fire service • Staff are advised to work from home	
7	All critical activities as stated in the BIA summary report	Pandemic/Epidemic i.e., COVID 19, SARD< EBOLA	<=1 hour <=4 hours	• Provision of hotel accommodation and security for critical staff (where necessary) • Activation of Business Continuity Plan • Employees revert to working from home or nearest branch • Provision of mobile data for employees • Provision of VPN for employees	• Mobile workstation • Internet data • VPN access
			<=12 hours <=24 hours	• Activation of Business Continuity Plan • Employees revert to working from home or nearest branch • Provision of mobile data for employees	

14.0 APPENDIX A – Plan Activation Contact Sheet

The following table should be used to record successful and unsuccessful initial contact with members of the IRT:

Name	Designation	Role in Plan	Mobile Number	Date/Time	Outcome (Contacted/No Ans /Msg Left /Unreachable)	ETA (if contacted)
Kingsley Oriere	Chief Risk Officer	Team Leader	0808 485 7704			
Jeremiah Adesina	Head, Operational Risk Management	Business Continuity Manager	0803 835 7868			
Damilola Essien	GH, Corporate Services	Facility Manager	0803 200 1862			
Kingsley Emekpe	GH, Central Operations	Incident Liaison	0705 600 4507			
Tolu Ogundipe	GH, Branch Services	Business Operations	0806 726 4370			
Ugo Ikonne	Chief Security Officer	Health and Safety	0803 083 9345			
Olanike Martins	GH, PMG	Human Resources	0802 370 7807			
Kenechi Obika	Head, Corporate Communications	Communications	0809 909 4061			
Chukwuemeka Nwaogu	Company Secretary & Chief Legal Officer	Legal and Regulatory	0809 651 1146			
Damilola Essien	GH, Corporate Services	Procurement	0803 200 1862			
Cosmas Uwaezuoke	Chief Compliance & Conduct Officer	Control	0805 590 3344			
Ayodele Shoyemi	Chief Financial Officer	Finance	0802 501 9937			
Myke Koledoye	Chief Information Officer	Technology	0803 154 9978			

15.0 APPENDIX B – Blank Activity Logging Form

Major Incident:		**Location:**		**Incident Team Leader:**	

Date	Time	Action	By	Comments	Signature

16.0 APPENDIX C – Blank Message Logging Form

Major Incident:		Location:		Incident Team Leader:	

Date	Time	Caller	Caller’s number	Message for	Message

17.0 APPENDIX D – Internal Contact Telephone Numbers

The following table shows the telephone numbers of key internal personnel:

Name	Designation	Role in Plan	Telephone Number	Email address
Kingsley Oriere	Chief Risk Officer	Team Leader	0808 485 7704	kingsley.oriere@premiumtrustbank.com
Jeremiah Adesina	Head, Operational Risk Management	Business Continuity Manager	0803 835 7868	jeremiah.adesina@premiumtrustbank.com
Damilola Essien	GH, Corporate Services	Facility Manager	0803 200 1862	damilola.essien@premiumtrustbank.com
Kingsley Emekpe	GH, Central Operations	Incident Liaison	0705 600 4507	kingsley.emekpe@premiumtrustbank.com
Tolu Ogundipe	GH, Branch Services	Business Operations	0806 726 4370	tolulope.ogundipe@premiumtrustbank.com
Ugo Ikonne	Chief Security Officer	Health and Safety	0803 083 9345	ugo.ikonne@premiumtrustbank.com
Olanike Martins	GH, PMG	Human Resources	0802 370 7807	olanike.martins@premiumtrustbank.com
Kenechi Obika	Head, Corporate Communications	Communications	0809 909 4061	kenechi.obika@premiumtrustbank.com
Chukwuemeka Nwaogu	Company Secretary & Chief Legal Officer	Legal and Regulatory	0809 651 1146	chukwuemeka.nwaogu@premiumtrustbank.com
Damilola Essien	GH, Corporate Services	Procurement	0803 200 1862	damilola.essien@premiumtrustbank.com
Cosmas Uwaezuoke	Chief Compliance & Conduct Officer	Control	0805 590 3344	Cosmas.uwaezuoke@premiumtrustbank.com
Ayodele Shoyemi	Chief Financial Officer	Finance	0802 501 9937	ayodele.shoyemi@premiumtrustbank.com
Myke Koledoye	Chief Information Officer	Technology	0803 154 9978	myke.koledoye@premiumtrustbank.com

18.0 APPENDIX E – Useful External Contacts

The following table shows the contact details of agencies who may be useful depending on the nature of the incident:

Name of Agencies	Address	Telephone Number
Federal Fire Service	Campus Lagos	017913929
Lagos State Fire Service	Lagos State Fire Service	01-744929, 08033235890
Onikan Fire Service	Onikan Opposite National Museum, Beside MUSON Center, Onikan, Lagos.	08186404240
NPA Fire Service	NPA Marina Lagos	07039715147
Julius Berger Fire Service	Julius Berger Company, Lagos	01-7755893
Federal Road Safety Commission	Federal Road Safety, Lagos	08033706639
LASAM BUS	Lasambus, Lagos	01-49798449
State Security Services (SSS)	Department State Service (DSS) Maitama, Abuja	08132222105-9
Nigeria Security and Civil Defence Corps (NSCDC)	Plot V921 Cadastral Zone A2, No 8 Algia Street Opposite High Court of Justice, Wuse Zone 5, P.M.B 301 Garki, Abuja	09-8767018, 09-8767019
Defence Intelligence Agency (DIA)	PMB 551, Asokoro, Garki-Abuja	09093500071, 08059694311

19.0 APPENDIX F – The Phonetic Alphabet

In order to ensure that messages are understood correctly, the phonetic alphabet should be used when spelling out words and numbers.

Phonetic Alphabet				
A – Alpha	B – Bravo	C – Charlie	D – Delta	E – Echo
F – Foxtrot	G – Golf	H – Hotel	I – India	J – Juliet
K – Kilo	L – Lima	M – Mike	N – November	O – Oscar
P – Papa	Q – Quebec	R – Romeo	S – Sierra	T – Tango
U – Uniform	V – Victor	W – Whiskey	X – X-ray	Y – Yankee
Z – Zulu	0 - Zero	1 – Wun	2 – Two	3 - Tree
4 – Fower	5 – Fife	6 – Six	7 – Seven	8 - Ait
9 – Niner				

The End