|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Document Configuration** | | | | |
| Document Title | | Business Continuity and Disaster Recovery Plan | | |
| Document Subject | | Business Continuity | | |
| Document Number | | Version 1.0 | | |
| Document Issue Date | | ddmmyyyy | | |
| Document Owner | | YYYY | | |
| Document Coordinator | | YYYY | | |
|  | |  | | |
| **Approval** | | | | |
| ***Name*** | ***Position*** | | ***Signature*** | ***Date*** |
|  |  | |  |  |
| Version Control   |  |  |  | | --- | --- | --- | | Version | Date | Description | |  |  |  |   This document contains confidential information and is the property oXXXX. Distribution is restricted to XXXX and restricted third parties as approved by the document owner. By accepting this document, the recipient agrees not to provide this document or any information contained therein to any third party without express prior written consent of XXXX. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without express or written permission of the Security Committee. | | | | |

Contents

[1. Introduction 3](#_Toc41391053)

[2. Purpose of the Plan 3](#_Toc41391054)

[3. Scope of the Plan 4](#_Toc41391055)

[3.1.1 Applicability to employees 4](#_Toc41391056)

[3.1.2 Applicability to External Parties 4](#_Toc41391057)

[3.1.3 Applicability to Assets 4](#_Toc41391058)

[4. Business Impact Analysis 4](#_Toc41391059)

[5. Crisis Management 5](#_Toc41391060)

[6. Emergency Procedures 13](#_Toc41391061)

[7. Business Recovery Plan 19](#_Toc41391062)

[8. Disaster Recovery Plan 25](#_Toc41391063)

[9. Enforcement 31](#_Toc41391064)

[10. Document Management 31](#_Toc41391065)

[10.1 Document Ownership 31](#_Toc41391066)

[10.2 Document Coordinator 31](#_Toc41391067)

[10.3 Distribution 31](#_Toc41391068)

[Business Impact Analysis Summary Report 33](#_Toc41391069)

[A key aspect of the Business Impact Analysis involved identifying the critical applications within each department and determining the impact of not performing the business process related to that application beyond the maximum acceptable outage 33](#_Toc41391070)

[The tables below summarize the number of applications rated as Critical, Essential, and Important, which are based on the recovery time frames determined by each XXXX department 35](#_Toc41391071)

[The full recovery plan for each department is listed in Appendix J 36](#_Toc41391072)

# Introduction

The Business Continuity and Disaster Recovery Plan for crisis management and orderly restoration of business activities upon the occurrence of an adverse event (e.g. a natural disaster or man-made disaster or technological failures).

It also establishes defined responsibilities, actions, and procedures to recover the XXXX’s computer, communication, and network environment in the event of an unexpected and unscheduled interruption.

# Purpose of the Plan

The purpose of a Business Continuity and Disaster Recovery Plan (referred to below as “BCP”) is to minimise interruptions to business activities and to ensure the availability and continuity of all services.  This plan will ensure that the XXXX can recover from disasters resulting in the partial or total loss of premises, IT infrastructure and applications to normal business operations, in a timely, effective and efficient manner.

The management of a serious incident is managed by the Security Committee (“SC” – see Appendix C for membership etc.), chaired by the CEO or by the COO in his / her absence. The SC will convene either “Face to Face” or by conference call depending on circumstances.

It is recognised that in the initial stages of some incidents, it may not be possible or practical for the SC to meet in which case the CEO, COO or other senior executive will direct the XXXX’s response until such time as the SC can meet.

The BCP will involve delivering on the XXXX’s contractual obligations whilst maintaining a minimal service, until such time as the XXXX re – groups and the SC can assess the situation in a controlled manner. The objective of this plan is to protect the XXXX and retain confidence of customers in the event of an undesired event or disaster.

This plan will enable the XXXX:

* To protect the lives of its employees;
* Minimize the disruption of operations and impact to customers using minimal resources;
* Provide an orderly recovery after a disaster;
* Guarantee the reliability of stand-by systems;
* Safeguard against any potential litigation;
* Preserve customer confidence; and
* Maintain competitive positions (at the discretion of the SC).

# Scope of the Plan

### Applicability to employees

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This plan applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant procedure statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This plan applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

# Business Impact Analysis

The Business Impact Analysis (BIA) shall highlight risk data about a Business processes and facilities and a plan to address the risk. The BIA which shall be created by the Business Continuity Manager shall consist of two parts:

* Business Impact Analysis (BIA)
* Corrective Action Plan

A Business Impact Analysis (BIA) describes the processes and sub-processes and the impact on the Business if they are interrupted.

**Processes**

Processes shall be defined at the Strategic Support / Business level. For each process, provide the following information:

* A description
* A Recovery Time Objective (RTO) and Recovery Point Objective (RPO) both expressed in terms of hours
* A Criticality Rating based on the Recovery Time Objective

**Sub-processes**

Sub-processes, which are defined at the departmental level, shall inherit the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) from the parent (Process). However, the Business Continuity Manager may override inherent risk values to enhance granularity of the risk rating.

Sub-processes require a description, sub-process Quantitative Value and Sub-Process Qualitative Value.

**Criticality Rating**

Use the following chart to establish a process or sub-process Criticality Rating when developing a Business Impact Analysis (BIA)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Criticality** |  |  | **RTO/RPO** |  |  | **Characteristics** |  |
|  | **Rating** |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 1 | |  |  | RTO < 4 Hours | |  | Minimal tolerance for downtime and Data | |
|  |  | RPO < 4 Hours | |  | loss | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  | |
| 2 | |  |  | RTO>4<24 Hours | |  | Limited tolerance for downtime and data | |
|  |  | RPO>4<24 Hours | |  | loss | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  | |
| 3 | |  |  | RTO>24<48 Hours | |  | Moderate tolerance for downtime and data | |
|  |  | RPO>24<48 Hours | |  | loss | |
|  |  |  |  |  |
|  |  |  |  |  | |  |  |  |
| 4 | |  |  | RTO>48<72 Hours | |  | High tolerance for downtime and data loss | |
|  |  | RPO>48<72 Hours | |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |
|  |  |  |  | RTO > 72 Hours | |  | Protracted tolerance for downtime and | |
| 5 | |  |  |  | data loss | |
|  |  | RPO > 72 Hours | |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Corrective Action plan (CAP)**

This contains plans to correct the gaps identified after the completion of the BIA. Business Continuity Manager is responsible for closure of Business Continuity CAPs.

A report on the BIA conducted is in Appendix N

# Crisis Management

**Crisis Management Team/Security Committee Engagement and Notification Levels**

The following impact levels shall assist in defining the severity of a Crisis Event and the appropriate Crisis Management Team or teams to support mitigation. The Security Committee is designated as the Crisis Management Team and Crisis Event levels are detailed below:

**Level IV**: Crisis Event Severity IV (Low impact)

* Couple of systems not working in the XXXX
* Lift not working

**Level III**: Crisis Event Severity Level III (Medium Impact)

* Office equipment like printers, scanners not working
* Biometric access system not working
* Unapproved changes to information or data or system hardware, firmware, or software characteristics

**Level II:** Crisis Severity Level II (High Impact)

* Downtime on the XXXX’s CBA for more than 6 hours but less than 24 hours.
* Malware attacking a couple of systems.
* Isolated fire incident in a unit of the XXXX e.g. fire incidents operations unit, treasury, treasury operations, etc.

**Level I:** Crisis Severity Level I (Critical Impact)

* Crash of the XXXX’s core banking application (CBA) or downtime on the CBA for more than 24hrs
* Malware attack on the XXXX’s system and network with associated failed recovery attempts
* Terrorist attack, fire incidence, disease spread, riots etc affecting the XXXX’s office.

The following crisis escalation template will be used to escalate Crisis Events



**Technical Service Teams**

Below are the technical service teams for the running of the Business Continuity and Disaster Recovery Plan

**Damage Assessment Team**

The site damage is assessed by the Damage Assessment Team at the department, which may be the floor or the whole head office. The primary thrust for this team is to do four things:

1. Report on the level of damage to operations and infrastructure of the XXXX to Security Team and Command Post.
2. Provide assessment of salvageability of major hardware components and other infrastructure.
3. Provide information for the Recovery.
4. Document the nature, scope, magnitude, location and level of impact

**Composition:**

1. Information Technology representative
2. Facilities/General Services representative
3. Brand & Marketing Communications representative
4. Human Capital Management representative
5. Operations Representative

**Recovery Teams**

The primary responsibility is to ensure continuity of business i.e. recovery at the Alternate Site and return to Primary Site. The main activities shall include:

1. recover processes
2. report into the Security Committee and Command Post
3. provide solutions on how to recover processes.

**Composition:**

i. Information Technology representatives

ii. Human Capital Management representative

iii. Brand & Marketing Communications representative

iv. Facilities/General Services representative

v. Operations Representative

**Functions during Recovery process:**

**a. Crisis Management Team/Security Committee**

1. Escalates to Executive Management Team to declare crisis.
2. Make a roll call using the call tree at the assembly point.
3. Notification Call List initiated.
4. Carry out staff categorization.
5. Identify sub-processes to be recovered first and others to follow

**b. Information Technology Team –**

Application Support Team; System Administrator Team; Network Enterprise Team; Network Support Team; Core banking Application Team: this part of the Recovery Team handles all information technology issues at the primary and alternate site.

**c. Human Capital Management Team**

This team segment should be designated to handle next of Kin or family contact. This person shall be available throughout the recovery process to aid employee’s family members.

**d. Brand & Marketing Communications Team**

This segment of the team handles publications / information dissemination to staff, customers, general public via the internet (social media, emails etc.), television, radio and dailies (magazines, newspapers etc.)

**e. General Services Team**

This segment needs to be familiar with the process of getting construction work scheduled and completed on time. The team should be able to understand and oversee the set-up of the electrical, environmental, and communication requirements of the Primary & Alternate Sites. The team should also be able to provide logistics – traveling arrangement, recall of battle-box, etc.

**f. Departmental Representative**

To ensure their respective departments information systems can be restored within the required time and to provide specialist support to the Team

**g. Business Continuity Manager**

The designated Business Continuity Manager will be the Head of Operations who will support all departments and functions in the implementation and execution of the Business Continuity Policy, Business Continuity Plan, Disaster Recovery Plan and Crisis Management Plans.

Responsibilities include:

1. Deliver to the XXXX Continuity of Business expectations.
2. Support the XXXX and departments as appropriate.
3. Develop and maintains Business and Disaster Recovery Plans to identify resources and services that are required by the business unit during a Business Interruption
4. Conduct due diligence to understand recoverability of third-party service providers in conjunction with vendor relationship managers and adjust planning accordingly.
5. Monitor and updates approved Continuity of Business tools with relevant Business Recovery Plans, documents and information
6. Prepare the Business Impact Analysis according to Continuity of Business Policy and Policy Standard
7. Coordinate and perform Testing of Business and Disaster Recovery Plans and Crisis Management Plans for their respective departments
8. Ensure any non-compliance is documented and resolved in a timely manner
9. Ensure independent Reviews of Business and Disaster Recovery Plans
10. Report metrics of Business Continuity program effectiveness.
11. Perform and documents test preparation, testing and post-test activities
12. Participate in the minimum number of pre-approved training activity as required by the Business Continuity policy and plan

**h. Internal Audit**

Responsible for independently assessing the effectiveness of BCP and DRP management processes and practices and providing timely objective assurance on the control of risk

**Crisis Event Documentation**

i. Event Log – Record of crisis event. This shall be prepared by Security Committee

ii. Event Impact Report – The impact of crisis event, damage assessment report that will be useful for Insurance claim. And the salvageable items recovered after crisis and after event

iii. After Action Review Report - this is a report that analyses effectiveness and efficacy of our plans and procedures i.e. Business Recovery Plan, Command Post, Crisis Management Plan, etc.

iv. Corrective Action plans.

v. Lessons Learned Report for Level II and Level I Crisis Events, these documents shall be forwarded to the Executive Management

**Crisis Management / Coordination Process**

Departments shall have or refer to Crisis Management Plans that include:

**Employee Response and Communication for Events occurring during Business Hours**

i. Evacuation and Assembly

Updates from General Services or facilities representatives are delivered to the assembly point.

In circumstances where staff assembly is practically impossible due to riot or unrest, the following shall be done:

a. Business Unit or Office Business Recovery shall contact the Crisis Management Team/Security Committee of the incidence and wait for further instructions to activate of Business Recovery Plan.

b. In situation where the entire area or city is affected by the unrest / riot, the Business Office at the alternative site at SunGard Availability Services (UK) Ltd, 38-42 Southwark Bridge Road, London SE1 9EJ can be used to continue operations for a few number of critical staff. The rest of the staff can work from home using the Citrix workspace

Major customers shall be contacted to inform them of our new base of operation pending when situation stabilizes.

Staff categorization shall be activated as follows in line with criticality of staff:

**Category 1** - Employees that shall relocate to a dedicated business recovery facility in the event of crisis i.e Sungard

**Category 2** - Employees that shall relocate to alternate sites in the event of crisis i.e a Third-party provider’s office like Frontier

**Category 3** - Employees that can work from a remote location using remote access capabilities.

**Category 4** - Employees that shall remain at home in a crisis event and not report to work and do not require remote access

**ii. Crisis Calling Procedures**

Hence, coordination among the crisis teams, update of staff and communication with external stakeholders are critical and should be managed by Brand & Marketing Communications.

These procedures may include pre-established telephone numbers for communication during the event. This could also include emergency telephone numbers of the XXXX.

The XXXX’s telephone number is below

|  |  |
| --- | --- |
| **S/N** | **EMERGENCY CONTACT NUMBER** |
| 1 |  |

Crisis or Disaster information received is communicated to any of the following below

a. Business Continuity Manager

b. Unit Heads

c. XXXX Emergency contact, see table above

**iii. Staff and Corporate Communication Procedures**

Plans to inform employees and keep senior management up to date on the status of a Crisis Event. Brand & Marketing Communications manage this process across the XXXX.

See below for steps to be tailored when crisis occurs during business hours:

**During Business Hours**

1. Respond to any alarm

2. Evacuate the building and go to emergency assembly point

3. Whilst at the assembly point, the Business Continuity Manager should follow the Crisis Calling Procedures – using the Call List & Call Tree, emergency number or SC

4. If Business Continuity Manager is unavailable, any designated staff should contact Crisis Emergency number/SC

5. If in situation you are unable to return to building, the Business Continuity Manager shall follow instructions of SC.

6. Be prepared to send staff home, and activate working from home through Citrix workspace till the situation improves.

**Employees Response and Communication for Events Occurring After Business Hours**

i. Staff and Corporate Communication Procedures

Plans to inform employees and keep senior management up to date on the status of a Crisis Event. Brand & Marketing Communications manage this process across the XXXX.

ii. In situation where staff other than the Business Continuity Manager have access to disaster information and do not have the Business Continuity Manager contact number, he/she shall call Zenith Emergency telephone number, which in turn informs Brand and Marketing Communications, which informs relevant persons or all employees, where applicable and keep senior management up-to-date on the status of the Crisis Event

See below for out of business hours emergency responses:

1. It is likely your Line Manager or a member of the SC will inform you of the incident. Ask what assistance you can provide.

2. Make a note of the telephone number of who called you.

3. Make a report back on actions requested of you e.g. damage assessment

4. Depending on the call (which may be an alert of a possible disaster), in which case you need to call the Business Continuity Manager.

5. If privileged to notice the disruption first, call the Business Continuity Manager immediately or Emergency telephone number

6. The Command Post managed by Brand and Marketing Communications informs and keeps management abreast with up-to date information and coordinate staff during crisis.

7. The Business Continuity Manager should follow the Crisis Calling Procedures using the Call List and Call Tree

**Crisis Communication Plan (CCP)**

Crisis Communication Plans (CCPs) shall use tools that include Call Lists and automated notification applications.

Call List, contacts of all critical persons associated with Continuity of Business, shall also form part of the Continuity of Business Plan documentation at the Continuity of Business Entity level.

There are two parts of Crisis Communication plan:

A. Internal CCPs shall detail communication among the following teams:

i. Executive Management

ii. Security Committee

iii. Employees who have local emergency facility and communications access rights.

B. External CCPs, shall be developed with input from Brand and Marketing Communications and Legal, include:

i. Regulators

ii. Markets and exchanges

iii. Media

iv. Customers

v. Shareholders

vi. Vendors, suppliers and other third-party services providers.

**Command post**

This is staffed by the Security Committee and Departmental Heads and shall coordinate XXXX staff during Crisis. Brand and Marketing Communications shall be primarily responsible for liaison with local police, fire and other external emergency contacts. Also, note the command post can be convened virtually.

1. Virtual location shall be equipped with Conference call number with domestic and international call numbers, leader and participant codes.
2. Each Command Centre shall be equipped with the following:

LAN connected PC

1. Intranet access.
2. Telephone.
3. Conference table with chairs.

**Composition of Command Post:**

1. Executive Management Staff
2. All Departmental Heads
3. Information Security Officer
4. Data Protection Officer
5. Facilities Officer

**Business Recovery Plan Activation**

Business Recovery Plan Activation information shall include:

1. Personnel authorized to activate the plan; this is the Head of Security Committee.
2. Protocol for notifying personnel and management of Business Recovery Plan Activation including Information Security considerations

**Note:** This is to be done after the situation has been stabilized.

**Plan Distribution**

Crisis Management Plan shall be made available to Security Committee members identified in the plan.

**NOTE:** The activation and assembly portions of the Crisis Management Planshall be made available to all employees.

# Emergency Procedures

**Safety**

This section covers emergencies that may occur at any time without warning like trip and fall, fire, electrical hazard, trapping in the elevator, utility disruption, bomb threat, and civil disorder among others and the safety procedures to be adopted.

**First Aid**

Each floor shall have a first aid box and be maintained regularly by facilities management.

**Roles and Responsibilities of Facilities Management on Health**

i. Management of First Aid Box

ii. Administration of basic First Aid Treatment

iii. Ensure that the First Aid Box is adequately stocked with basic medications

iv. Ensure that all expired drugs are not retained in the Box

v. Maintain current emergency telephone numbers for Doctors and Ambulance services

**Accidents - Medical**

1. Medical emergencies that require immediate attention may occur from time-to-time. Some examples of medical emergencies are dislocations or fracture, severe pain, bleeding of a severe nature, abnormal appearance of skin colour, fainting, unconsciousness, seizure, airway obstruction, cardiac arrest, pulmonary arrest, stroke, burns, diabetic coma, immobility, sudden swelling or hives, and absence of breathing. Any of these symptoms could be life threatening, a call to 999 should be made immediately and the following can be done to assist the victim till paramedics arrive
2. If the person is conscious, he or she shall be assisted to a comfortable position to enable him or her explain what really happened.
3. Where there are no signs of breathing, artificial ventilation and /or cardio-pulmonary resuscitation using the mouth-to-mouth or nose-to-mouth method shall be initiated.
4. If the staff is unconscious but he or she is still breathing and the airway is not obstructed, other staff present shall assist to lay the staff on his or her back and tilt the head backwards, slightly elevating the neck to establish and maintain an open airway. The feet shall also be elevated slightly.
5. Where the person is bleeding severely, direct pressure shall be applied to the wound or finger pressure to a pressure point.
6. If the injured person is an employee of the XXXX, brand and marketing representative shall locate the family profile and contact the next of kin to review any special treatment that may be needed, obtain the name of the employee's family doctor and determine the kind of treatment to be administered

**Trip and Fall**

Trip and fall are the major reasons given for most injuries in the office environment. In many instances, the causes are loosened or torn tiles, electrical and telephone cords or use of a chair in place of ladders or step stools. To avoid these issues:

1. The tiles shall be routinely checked for buckling or wear.
2. Substitution of electrical cords for permanent wiring shall be avoided. Employees shall be directed to always use the length of cord that is necessary to do their job and keep all cords from around their desk and chair areas.
3. Cords shall be secured to the floor or tiles where possible.
4. Heavy materials such as paper or storage boxes shall be stored on the lower shelves in the cabinets. The justification for this is that when retrieving these materials from lower areas, injury and falls are less likely to occur.
5. Files and desk drawers shall be closed when not in use. When filing or retrieving material from the cabinet, only one file cabinet drawer shall be opened at a time to prevent the cabinet from falling or tipping forward.

**Fire**

1. The most important issue in case of a fire emergency is evacuation of personnel from the building. Customers and employees, while remaining calm, shall be escorted to a safe and secure location.
2. Facilities Management shall contact the fire department or the Police where it is considered necessary.
3. Any action that may endanger human life shall be avoided.
4. All employees shall gather at a designated safe location to determine the severity of the incident.
5. Employees shall evacuate the building at the exit (stairs) nearest to their work area and walk calmly in single-file, assisting anyone in need of help. The use of the lift should be avoided.
6. Designated Fire Wardens shall have the responsibility of checking the toilets, conference rooms, and storage rooms for personnel or customers during the evacuation.
7. When outside the building, all employees, customers and visitors shall walk calmly to the designated area. All supervisors shall make sure everyone is accounted for by taking a roll call.
8. Once employees, visitors and customers are out of the building, they shall stay out. Only authorized personnel shall be allowed into the building for any reason until the authorities and / or the security representatives gives clearance.
9. Employees shall not discuss the disaster situation or evacuation procedure with anyone outside the XXXX. All questions should be directed to the Head, Brand and Marketing Communications
10. Staff shall be trained on emergency safety procedures.
11. There shall be periodic servicing and testing of firefighting equipment - fire extinguishers, water hoses, smoke alarms etc.

**Electrical Hazards**

1. Electrical hazards can be eliminated in office areas by adopting the following procedures:
2. Water and electricity do not mix. All employees shall avoid dampness or water on electrical equipment.
3. All employees shall ensure that electrical circuits are not overloaded by using multiple plug converters. They shall make use of strip outlets with a fuse or circuit breaker.
4. All employees shall ensure that all electrical appliances are switched off daily at the close of business. Duty officers shall ensure that this has been carried out before departure.

**Trapped in the Elevator**

1. Where a staff is trapped in an elevator, he or she is advised to be calm and know that he / she is protected inside the lift as the elevator will not fall down the shaft and nothing heavy can fall on the trapped person.
2. Where the light suddenly goes off or the elevator stops, occupants shall be advised to be patient and call the reception on any of the telephone or extension lines pasted on the wall of the elevator.
3. Facilities management shall initiate rescue operation as quickly as possible and advise the trapped employee as to how the rescue operation will be carried out.

**Utility Disruption**

1. In cases of short-term power outage, facilities management shall direct and assist personnel in all phases of actions that are required (see below).
2. Activate the emergency kits for flashlights, and portable radio with batteries.
3. Unplug all electrical equipment (computers, audio-visuals, projectors, etc.) and shut off all light switches. When power is restored, it may return in a surge and blow out light bulbs and other equipment.
4. If necessary, consider posting signs that read, “Temporarily closed due to power outage - sorry for the inconvenience.”
5. Where the cause of the power outage cannot be determined and the lighting is sufficient, all exits and entrances shall be locked for security purposes while they continue working or closed temporarily until the power is restored, depending on safety conditions for the employees.

**Bomb Threat**

1. Brand and marketing management, shall call 999 and notify the police bomb squad unit
2. Facilities management shall activate evacuation procedures immediately.
3. Unusual boxes and packages or items that do not seem to be appropriate to their surroundings shall be pointed out to the police.
4. Employees shall not touch or carry suspicious objects. They shall handle all familiar objects carefully and with caution.
5. The location of any suspicious object shall be reported to the police or security representative.
6. Facilities management shall direct all staff to move away from the immediate vicinity of the suspicious object.
7. If directed by the police or security officers, supervisory personnel shall begin to move any cash and vital records to the vault for secure storage.
8. If the police or security representative issues instructions to evacuate the area, all personnel shall keep calm and evacuate the building by using the nearest exit and go to the designated primary location to assemble so that supervisors or department heads can make sure everyone is accounted for.
9. Once employees, visitors and customers are out of the building, they shall stay out. No one shall be allowed back into the building for any reason until the "all clear" signal is given by the police.
10. Employees shall not discuss the evacuation procedure with anyone outside the XXXX. All questions posed to employees shall be referred to the spokesperson who will be the Head, Brand and Marketing Communications.

**Civil Disorder**

1. Where there is a case of civil disorder or protests in the vicinity of the business office, Crisis Management Team should immediately convene to decide on the next steps.
2. Employees shall not, under any circumstances, confront the protester(s) either physically or verbally or join the protest.
3. Where the disorder has elevated to a riot and destruction, staff shall secure all critical data, documents, etc., in a vault or fireproof storage area and evacuate the premises immediately with caution and under the guidance of the Security Committee, immediately it is safe to do so

**Natural – Tornado, Hurricane, Windstorm**

Security Committee will be kept aware of adverse weather conditions by radio and television, and will advise staff in the event of severe weather issues at hand. The following precautions will be taken:

i. If advised by senior management, secure all valuables, lock the doors and move to the lower level.

ii. Move away from outside walls and windows and go to the centre of the building.

iii. If any damage has occurred, inform facilities management

iv. DO NOT GO OUTSIDE OF THE BUILDING WHEN THREAT OF SEVERE WEATHER IS PRESENT / IMMINENT.

v. If feasible, the Management may consider either closing the XXXX early and permitting employees to leave early or permit late arrivals to accommodate for the severe weather conditions. If a state of emergency is declared and staff are consequently unable to commute to work, remote access working option should be activated.

**Natural - Earthquake**

During the Earthquake

All employees to do the following:

i. Take cover underneath a desk, table or doorframe.

ii. Stay away from windows and objects that could fall on you.

iii. Stay where you are and do not run outside due to falling debris.

iv. Do not use the elevator.

v. If you are outside, stay in an open area and do not enter the building.

vi. Do not use matches or open flames for light?

After the Earthquake

All employees to do the following:

1. Go to the inner-most-part of the building.
2. Be prepared for aftershocks.
3. Check telephone handsets that have been shaken off, but do not try to use the telephone except to report fires or medical emergencies. (If telephones still work, they will be needed for emergency communication.). Wait for and follow instructions from the security committee.
4. Give first aid to any injured personnel.
5. DO NOT MOVE INJURED VICTIMS UNLESS ABSOLUTELY NECESSARY.
6. Alert team leads and/or team members to anything needing their attention and are prepared to evacuate to lower floors if necessary.

**Man made – Extortion / Terrorist**

Extortion

Extortion is the act of demanding money using a threat. The demand may involve threats against persons or property. If you receive an extortion threat, do one of the following:

i. Document the words of the extortionist.

ii. Inform your Head of department/Executive Management.

iii. Executive management to report to the police

**Terrorist Threat**

A terrorist threat is an act, which is intended to force or intimidate someone to do something or punish them for having done something based on a threat of violence. The threat may be repeated to an individual or a group. Terrorist threats often involve bomb threats, threats to burn buildings, or threat to take action against a person or a group of people. If you receive a terrorist threat, do the following:

i. Write down the threat or demand that was made.

ii. Inform your Head of department/Executive Management

iii. Executive Management to report to the police

**Systems - Vendor Failure**

On an annual basis, financial analysis of all service providers of mission critical systems are conducted. For any service provider that exhibits any potential problem with respect to solvency, which may result in the threat of disruption of services provided to the XXXX, the XXXX may request to make arrangements that will guarantee the XXXX’s continuation of services. Options that the XXXX may take include, but are not limited to:

i. Placement of source codes in escrow held by a third party (Note: Such an arrangement has been made with Financial Objects);

ii. Back-up arrangements with another service provider of at least equal service quality.

**Systems – Information and Cyber Security Failure**

The XXXX shall take all steps to ensure information assets are well protected from unauthourised access both logically and physically. In case of information and cyber security incident affecting the XXXX’s operations, the XXXX will follow the steps as stated in XXXX-PRC-ALL-006 - Incident Response Procedure.

**Systems – Information Assets Failure**

The XXXX shall take every step to ensure all her information assets are adequately maintained and regular updates and patches done. In the event of a major systems failure where the given system cannot operate at the desired level leading to an incident, the XXXX will follow the steps as stated in XXXX-PRC-ALL-006 - Incident Response Procedure.

**Communicable diseases and Pandemic**

The XXXX’s executive management will review government directives on the communicable disease and pandemic and act according to the government directives to protect both the XXXX staff and XXXX’s operation.

**Alternative Working Arrangement**

For all the above scenarios, the default alternative recovery worksite is that Staff will be allowed to carry out their work functions from home using the Citrix workspace till executive management deemed it safe for normal activities to resume. Also, based on management decisions, some functions which must not be more than five staff can work out of the Sunguard disaster recovery centre.

# Business Recovery Plan

Business Recovery Plans (BRPs) are prioritized based on their Criticality Ratings, which are determined by the Criticality Rating of the highest rated sub-processes listed in the Business Recovery Plan. BRPs shall be documented and executable based on supplied versus demanded Recovery Time Objective.

**Planning Assumptions**

In developing a Business Recovery Plan, the following assumptions shall be used:

1. Use the Worst-Case Scenario
2. Consider dependencies on processes whether they are internal to XXXX or are provided by Vendors suppliers or other third parties

**Business Recovery Process**

The Business Recovery Plan shall contain the following elements if applicable or indicate if the element is not applicable:

**Sub-Process Recovery Strategies and Requirements**

Recovery strategies shall include:

1. Relocate to a disaster recovery site
2. Shift workload to an alternate site.
3. Initiate remote working procedure.
4. Do not recover

Resource requirements include staff, telephones, market data, and applications, printers, filling cabinets and paper / writing materials. The need for these resources in the Business Recovery Plan is listed in hours after interruption. For example, 20 telephones might be required to be recovered over 24 hours after the interruption. Show how many telephones are needed at each hour after the interruption.

The full recovery steps are in Appendix A: IT Recovery Checklist

**Call List**

A Continuity of Business document that describes the calling responsibilities and the calling order used to contact management employees, business recovery team, information technology recovery team, internal and external customers, Vendors, suppliers, and other third-party contacts and Crisis Management Teams.

The full call list is below

IT Recovery checklist and flowchart

Contact details for Public Services

SC Members, IT Team and Non-Executive Directors Directory

Workplace Recovery Inventory

Evacuation and recovery process

Suppliers

Important Contact Details

Staff Contact List

Departmental Recovery Plans

**Departmental Recovery Plan**

Department should identify and list their vital resources for recovery procedures:

1. Electronic items – process owners shall provide link to the share-drive where documents are stored.
2. Computer systems and application required should be specified, also number of minimum staff should be included.
3. For physical documents the process of retrieval is specified i.e. where documents are stored, contact person and special retrieval process. Copies of physical forms and templates copies are kept in the battle-box.

Each department recovery plan is listed in Appendix J: Departmental Recovery Plan

**Testing**

XXXX shall develop a Continuity of Business testing strategy, which contains seven elements:

1. Assumption
2. Objective
3. Success criteria
4. A master testing calendar
5. Test preparation
6. Testing
7. Post-test activities

This is to ensure that:

1. the plans are functional, fully documented and current
2. Staff, equipment and systems are in place
3. The test can be successfully audited

There shall be four types of tests:

1. **Table-top**: This is a review of Business Recovery Plan documentation.
2. **Standalone**: This is a test of a single plan component, which is a part of theBusiness Recovery Plan that can be tested in isolation. Examples Call Tree, Call List, Sub-process recovery strategies, Process risk identification etc.
3. **Component**: This is test of multiple dependent plan components whichtogether make a full Operational test example Technology recovery test
4. **Operational**: A complete test of Business Recovery Plan. An operational Testmay include simulations, technology solutions, and Manual Workarounds, Interaction between multiple teams may be tested during Operational Test. Multiple Standalone or Component Tests can be equivalent to a full Operational Test if they test all sections of the Business Recovery Plan. Note that other than Call List Testing much of crisis management testing is the verification of crisis management documentation using walkthrough techniques that prove that the Crisis Management Plan is executable.

**Master Testing Calendar**

Testing frequency shall be primarily a function of the underlisted type of test

1. An Operational test shall be conducted every calendar year for all Processes that have criticality rating 1 & 2 while those with criticality rating 3 to 5 shall be tested every 3 years.
2. Call Lists shall be tested twice per calendar year, once in the first half of the year and once in the second half.
3. Crisis Management Plan tests shall be conducted every calendar year and consist of verifying that Crisis Management Plan documentation is executable.

**Note**: Any tested component or components that fail shall be retested within120 days after the test. If a Business Recovery Plan is updated due to a material change, the affected sections shall be tested within 120 days after the material change.

**Testing Strategy**

Each department creates a testing strategy, which shall provide detail for testing applications and business processes that include test objectives, success criteria and methods for review and reporting of the test results.

**Assumptions** 45

At a minimum, testing assumptions shall include the following:

1. Considering the volume and function as well the Criticality Rating of the processes.
2. Validation of the availability and adequate of resources.
3. Coverage of all aspects of the Business Recovery Plan and satisfy recovery strategies.
4. Coverage of applications and supporting data included in the Business Recovery Plan. All applications must be tested annually.
5. Consideration of dependencies on processes which are external to the Group, whether they are internal to Zenith or are provided by Vendors, suppliers or other third parties.

**Objectives**

At a minimum, testing objectives shall include the following:

1. Plans are functional.
2. Tests do not jeopardize normal business operations or affect customer privacy

**Success Criteria**

At a minimum, success criteria shall include the following:

1. Recovery Time Objective requirements are met
2. The business process is functional

**Test Preparation**

**The following steps shall be adopted in test preparation**

1. Assess the process risks
2. Document and validate test scope including Recovery Time Objective, assumptions, objectives and success criteria.
3. Identify and resolve pre-test issues.
4. Develop test scripts that do not affect the integrity of production / live data.
5. Document logistics for test staff and vendors.
6. Identify test participants including any required participants from Process Owners, Business Continuity Management, IT Information security, Operational Risk Management and Vendors.
7. Work with internal and external vendors to ensure readiness of the test environment (examples include IT, and facilities management).
8. Write a test plan that identifies tasks and resources.
9. Document manual workaround procedures

**Testing Execution**

1. Execute test scripts.
2. Maintain an event log of activities and issues during the test.

**Post-Test Activities**

1. Validate testing objectives have been met.
2. Determine which test components have passed or failed.
3. Conduct an After Action Review (AAR), if required.
4. Prepare a Lessons Learnt Report within 30 days of the test.
5. Assign ownership for resolution of test issues by completing a Corrective Action Plan (CAP). Any retest that is not compliant is subject to Exception Process.

**Note:** Test results and any CAPs shall be used to update the BusinessRecovery Plan.

**Crisis Event Used as a Test**

An actual Crisis Event shall substitute for a test if the following requirements are met:

1. Enough component of the Business Recovery Plan was activated.
2. Supplied Recovery Time Objective met demanded Recovery Time Objective and is shown in the documentation.
3. Business Unit Head approved the documentation
4. An After-Action Review (AAR) was conducted.
5. A lesson learnt Report was prepared within 30 days of the event.

**Note:** Any test objectives not fulfilled by the Crisis Event shall be testedas would normally be required.

**Maintenance**

Maintenance shall be performed at least once a year on Business Continuity and Disaster Recovery plan

Maintenance shall be initiated by any of the following Continuity of Business Maintenance Triggers:

1. New calendar year
2. Updates to the Business Continuity and Disaster Recovery plan
3. Major change in the XXXX’s strategy or business line
4. Application or related changes e.g. new XXXXing application
5. Independent Review - internal or external
6. Business Recovery Plan Test
7. Crisis Management Plan Test
8. After a material change in Business Merger, Acquisition or Divestiture, a significant reorganization or a change in facilities, staffing of technology infrastructure that renders part or all plan obsolete.
9. Revision triggered by regulatory requirements
10. Actual Crisis Event or Business Interruption that identifies items that require review in conjunction with the Exception Process

**Monitoring and Reporting**

Adherence to regulatory requirements including FCA, ISO 27001, Basel II, and MiFID as well as reporting appropriate reporting of operational risks to senior management and the Board of Directors.

**Key Continuity of Business Metrics**

All departments shall report Key Continuity of Business Metrics regularly (half yearly). These metrics related to important risks shall include:

1. Business Impact Analysis
2. Crisis Management Plan
3. Business Recovery Plan
4. Testing
5. Corrective Action Plans
6. Exceptions or deviations
7. Independent Reviews
8. Training
9. Audit issues

**Exception Process**

Exceptions to this Policy shall be submitted to Chief Operations Officer and shall be approved by the Security Committee for the business requesting the Exception.

If an exception has a criticality impact rating of 1 (critical) or 2 (high) the Security Committee shall also approve the Exception. All Exceptions shall be forwarded to Security Committee for tracking, metrics and assignment of the Exception ID. For Medium and Low, shall be forwarded in writing (email or scanned images) to Chief Operations Officer. The Exception Form shall be updated and approved for extensions greater than one year.

**Communications**

**Customer Inquiries**

The Head Brand and marketing shall develop a standard response letter for customer inquiries about Zenith Continuity of Business Program. Businesses may amend the response letter to comply with their local regulatory and legal requirements after consultation with the Security Committee.

**Presentations, Shareholder Communications and Marketing Materials**

Continuity of Business-related information prepared for external presentations, Shareholder Communication and Marketing materials shall be reviewed by the Security Committee and the company’s Legal Adviser prior to release. The Security Committee shall review any presentations that include Business Continuity Policy and Standards. The publication shall be authorized by the CEO in line with the provisions in the XXXX External Communication Policy as approved by the Board of Directors.

**Insurance Risk Management**

Security Committee shall liaise with the Legal department to confirm appropriate insurance cover is available for our assets.

**Training**

The Business Continuity Management shall make available a set of core Business Continuity Planning training activities and classes.

It is recommended that all other personnel with Continuity of Business-related responsibilities complete a minimum of one training activity per year.

50

**XXXX Business Continuity Policy**

**Corporate Training Program**

Courses shall include training for the following:

1. Continuity of Business Governance
2. Conducting Business Impact Analysis
3. Building and executing Crisis Management Plan
4. Building and executing Business Recovery Plan
5. Testing a Crisis Management Plan and Business Recovery Plan
6. Maintaining Crisis Management Plan and Business Recovery Plan
7. Continuity of Business Policy and Policy Standards
8. Monitoring and Reporting requirements
9. Legal and regulatory guidelines

**Training Delivery**

Training shall be delivered in the following ways

1. General awareness and sensitization
2. Classroom instruction
3. Web-based through E-Learning
4. Video presentation
5. External certification program or Continuity of business-related courses
6. Workshop and training exercise

# Disaster Recovery Plan

**Introduction**

The management of the XXXX recognizes and understands the dependence of the business on technology for service delivery across and the potential loss of revenue and operational control that may occur in the event of a disaster; has prepared this comprehensive disaster recovery plan as part of a larger business continuity plan.

The intent of this Disaster Recovery Plan is to provide a written plan directing the technology system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster. Restoration of critical servers will follow the Zenith DR Invocation Test Plan v1.0 listed in the Appendices

The Disaster Recovery Plan preparation process includes several major steps as follows:

1. Identify Systems and Applications currently in use
2. Analyze Business Impact of technology downtime
3. Determination of critical recovery time frames (Recovery Point Objective and Recovery Time Objectives)
4. Document Recovery Team Organization and Responsibilities
5. Develop and Document Emergency Procedures
6. Document Training & Maintenance Procedures
7. These steps were conducted and this document represents the completed effort in the preparation of the Disaster Recovery Plan**.**

These steps were conducted, and this document represents the completed effort in the preparation of the Disaster Recovery Plan**.**

**Disaster Recovery Project Approach**

In defining the appropriate solution, the XXXX defined the minimum considerations the ideal option must meet to include:

1. Minimal impact on current and future cash flow projections
2. Total cost of ownership (short to long term)
3. Low to medium lead time to setup
4. Present realities in the Industry
5. Technology trends (Virtualization, Cloud Computing)

The items formed guiding principles for developing the solution design and assessment process. The assessment process adopted a three-step approach to arrive at the recommendations presented on the next page.

The process began with a detailed requirement gathering phase which basically researched global trends, IT standards and prevailing industry practice around setting up a disaster recovery site. This process provided useful input into functional and technical requirements specification for this project.

This step was followed by site selection using a discovery process which involved sending out requests for information to all available sites with collocation services. All the information obtained from this process fed into the solution design step in which scenarios and options were created from the combinations of different factors and approaches.

At the end of this process the XXXX approach is summarized below:

1. Explore options around hosted services to reduce the capital expenditure and required lead time to launch a live site
2. Adopt a phased approach to achieving full business continuity of technology platforms prioritizing key line of business applications with the highest impact on customer service delivery across all our touch points.

**Technology Platform Impact Analysis**

The focus with respect to planning for disaster recovery for us is time sensitivity and criticality. As such technology platforms have been assigned sensitivity ratings of 1 to 3 with 1 being the highest and 3 being the lowest based on the impact per second of downtime on service channels and consequently income generation.

The applications listed below include the availability of dependent infrastructure (servers, storage, connectivity, power).**Recovery Objectives**

Recovery Point Objective and Recovery Time Objectives which are critical factors which determine significant aspects of the backup strategy, approach and technology are determined strictly by business and regulatory requirements.

* **Recovery Time Objective (RTO)** is the duration of time and a service levelwithin which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. It includes the time for trying to fix the problem without a recovery, the recovery itself, tests and the communication to the users.
* **Recovery Point Objective (RPO)** describes the acceptable amount of dataloss measured in time. The Recovery Point Objective (RPO) is the point in time to which you must recover data as defined by your organization. This is generally a definition of what an organization determines is an "acceptable loss" in a disaster situation.

The recovery grid below describes the Priority of each data category based on the RTO and RPO as defined by business requirements

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | **RECOVERY POINT OBJECTIVE** | |  |
| **RECOVERY TIME** |  |  |  |  |  |
| **OBJECTIVE** |  | **Within 1 Hour** | **Within 24 Hours** | **>24 Hours** |
|  |  |  |  |
| **Within 1 Hour** | Impact 1 | Impact 1 | Impact 1 |
|  |  |  |  |
| **Within 24 Hours** | Impact 1 | Impact 2 | Impact 3 |
|  |  |  |  |
|  |  |  |  |  |  |
|  |  | **> 24 Hours** | Impact 1 | Impact 2 | Impact 3 |
|  |  |  |  |  |  |

Based on these recovery objectives, all services have been classified with recovery objectives based on the perceived impact.

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **Application** | **Use** | **Criticality** |
| 1 |  |  | 1 |

**Back-Up and Replication Strategy**

In line with the RTO, RPO and impact analysis done above, the backup strategy will be online replication: This is basically hot replication of all application data between the live site at Milton Keynes and the offsite data centre in Maidenhead.

**Recovery Organization**

The effectiveness and operability of the Disaster Recovery Plan is dependent on the knowledge and expertise of the personnel who develop and execute the plan. A recovery from a disaster is best conducted by teams of personnel that are formed to perform specific functions (e.g. infrastructure / applications management).

The organization of the staff to recover the system is designed for the worst-case situation. The worst case, requiring a move to the alternative site, must be executed by a coordinated team to minimize the operational impacts to end-users, senior management and the XXXX.

The Disaster Recovery Team Organization, therefore, is set up to accomplish:

* Expeditious and efficient recovery of transaction processing.
* Intermediate and minor impact/expenditure decisions within the Information Technology personnel during the recovery process.
* Major impact/expenditure decisions at the management level.
* Streamline reporting of recovery progress from recovery teams upward to senior management and end-users.

The Disaster Recovery Manager (DRM) in charge of the Disaster Recovery Team will be the Head of IT and reporting to the Security Committee. All IT staff will be members of the recovery team The DRM will have the following responsibilities

1. Supervisory oversight of the recovery process and to work with all the IT staff to achieve the listed tasks
2. Ensure migration of all departments to the DR site for transaction processing
3. Setup tack team at recovery site for responding to user issues
4. Setup incident team at recovery site for responding to user issues
5. Communicate with link providers to manage and redirect link traffic
6. Provide alternate communication channels for internal communications
7. Ensure suitability and availability of recovery site
8. Ensure physical security of assets and human resources

The following steps will be taken to restore services in the event of a disaster:

* Notify all link vendors of disaster and instruct vendors to migrate branch links to the disaster recovery site.
* Activate all impact 1 services for active processing.
* Requisition infrastructure for impact 2 services.
* Install infrastructure at disaster recovery site.
* Restore impact 2 applications and services to new hardware from backup devices.
* Advice users on availability of platforms

**Operational Recovery vs. Disaster Recovery**

Procedures to rectify disruptions to normal operations as a result of temporary unavailability of service dependents is categorized as operational recovery, the failure to rectify disruptions within acceptable time frame shall necessitate escalation to disaster recovery measures. The downtime threshold shall de defined on scheduled review of this document per business division.

Each defined business unit must be properly equipped to monitor resources and detect disruptions to their products and service dependents, units and divisional heads shall be direct recipients of all alerts and reports. In the absence of such tools, business processes must be created solely for monitoring and reporting purpose.

For each business unit designated as critical, there must be duplicity of required equipment at alternate locations while assigned to other business units during normal periods.

**Evasive Action**

In the event of an escalation of a service disruption to disaster status, all operations dependent on the affected service(s) should be halted immediately.

Each service should be assigned an administrator, this administrator is mandated to confirm or otherwise the veracity to claim disaster status for a service or product.

**Team Management / Coordination**

Each business unit is mandated to designate unit member as a disaster recovery officer with a subordinate in acting capacity. It is therefore mandatory that one of the nominees must always be present or reachable by unit members.

Personnel positions mandated to operate equipment or administer services designated as critical must be duplicated. Human Resource shall be mandated to verify the suitability of all nominated officers and subordinates nominated by the unit heads.

**Evacuation & Relocation**

Evacuation of personnel from each business unit shall be the responsibility of the disaster recovery officer; each unit member shall be accounted for on exit and communicated to the unit head.

Equipment designated as critical, but immovable shall be labelled appropriately for identification during physical recovery.

Unit member relocation to battle stations (recovery site) shall be at the coordinated by the disaster risk officers and shall not exceed the allocated number of personnel in Appendix J: Departmental Recovery Plans

**Succession Plan**

The succession plan of XXXX shall clearly state the principal officers for divisions, departments, and units in the XXXX. It shall also articulate the first and second level relief officers to these principal officers. This is to ensure that for every unit and function in the XXXX, there is someone else available to effectively manage the responsibilities inherent in the function if unforeseen circumstances render the principal officer incapable of executing his/ her responsibilities.

Appendix J: Departmental Recovery Plan, shows the head of each department and other officers supporting the head.

# Enforcement

As noted above, this applies to all staff, officers, members of the Board of Directors, and all consultants and contractors. Violations of this document may result in disciplinary action, up to and including termination of employment and / or legal action.

# Document Management

## Document Ownership

This is owned by the YYYY

## Document Coordinator

This is coordinated by the YYYY

## Distribution

* *All staff*

# Appendix N: Business Impact Analysis Summary Report

**1.0** **Executive Summary**

The goal of the Business Impact Analysis report is to develop a prioritized list of business recovery targets that become the focus of subsequent recovery strategies. The BIA provides the foundation for developing well-reasoned and prioritized responses. Since the resources of the Authority are limited, the BIA analysis will help to ensure that the subsequent IT Business Continuity/Disaster Recovery Plan is focused on reestablishing the most critical resources in the most cost effective manner to minimize loss and disruption resulting from a potential disaster event.

**2.0** **Outage Impact Summary and Application Analysis**

The business impact analysis involved identifying the critical business processes and related supporting resources within XXXX departments and determining the potential impact of an outage or disruption in services. The process included a comprehensive assessment of all business activities that are performed within XXXX departments, as well as an analysis of the supporting resources that are required to perform these activities. This includes support in the form of servers, network, PCs, communications, facilities, systems software, and applications software.

A key aspect of the Business Impact Analysis involved identifying the critical applications within each department and determining the impact of not performing the business process related to that application beyond the maximum acceptable outage

**2.1** **Impact Levels**

The department’s used the following categories to rate the impact of an application outage to performing their related to business processes:

* Department Operations
* Financial/Economic
* Customer Service
* Safety/ Health
* Statutory/Regulatory

**2.2** **Application Analysis**

The following information was gathered and analyzed for each software application:

* Maximum Outage (period of time the business process that uses the application could be deferred) as determined by the users
* Availability of Alternate Processing Methods such as manual procedures
* How often (cycle) the application is used (i.e., daily, weekly, etc.)
* Duration (length of time) that the alternate process could be performed
* Volume (# of transactions per cycle)
* Potential Litigation

The result of the outage impact analysis is summarized below.

This summary information is useful in understanding the rational for the criticality of the specific applications identified by the departments.

**3.0** **Application Priorities and Recovery Time Frames**

Following an interruption to the business processes for a department, resumption activities need to be focused on those processes that once lost, would significantly impact the ability to perform critical business processes. While recovering all business activities is the ultimate goal of an IT Business Continuity/Disaster Recovery Plan, critical systems and applications must be restored first to minimize the impact on essential operations. The software applications were identified and compared based on:

* Deferral period (period of time the process could be deferred) as determined by the users
* Availability of alternate processing methods such as manual procedures
* Duration (length of time) that the alternate process could be performed
* Potential litigation
* Potential revenue losses
* Operational impact
* Financial / economic impact
* Customer service
* Public safety / public health
* Regulatory / statutory impact
* Other factors

The applications identified by XXXX .’s departments were assigned a rating based on the following criteria listed below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Ranking** |  | **Description** | **Recovery Objectives** |
|  |  |  |  |
| **Critical (1)** |  | **Application must be restored within 1 day or less** | **One Day or Less** |
|  |  |  |  |
| **Essential (2)** |  | **Application must be restored within two days** | **Two Days** |
|  |  |  |  |
| **Important (3)** |  | **Application can be restored after 3 or more days** | **Three or More Days** |
|  |  |  |  |

The tables below summarize the number of applications rated as Critical, Essential, and Important, which are based on the recovery time frames determined by each XXXX department

|  |  |  |  |
| --- | --- | --- | --- |
| **S/N** | **Application** | **Use** | **Criticality** |
| 1 |  |  | 1 |