RÉPUBLIQUE DU SÉNÉGAL

Un Peuple – Un But – Une Foi



MINISTERE DE L'ENSEIGNEMENT SUPERIEUR, DE LA RECHERCHE ET DE L'INNOVATION

****

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR





****

ECOLE SUPERIEURE POLYTECHNIQUE

****

DEPARTEMENT DE GENIE INFORMATIQUE

****

MÉMOIRE DE MASTER INFORMATIQUE

Spécialité : Management de le Sécurité des Systèmes d'Information

Sujet : Mise en place d'un plan de continuité d'activité en milieu bancaire : cas de la banque atlantique Togo

Présenté et Soutenu publiquement par :

M^me^ DILLE DJAMILA

Encadré par Dr. Chérif DIALLO et Dr. Khadidiatou Wane KEITA

Le : 13 / 10 / 2021

Jury :

Président :	Pr. Amadou Thierno GAYE	Professeur Titulaire, ESP
Examinateur :	Dr. Doudou FALL	Maître Assistant, ESP
Examinateur :	Dr. Cherif DIALLO	Maître de Conférences, UGB
Examinateur :	Dr. Khadidiatou Wane KEITA	Maître de Conférences, ESP

Année universitaire 2019/2020



Un Peuple – Un But – Une Foi

RĒPUBLIQUE DU SENEGAL

UNIVERSITĒ CHEIKH ANTA DIOP DE DAKAR

ĒCOLE SUPĒRIEURE POLYTECHNIQUE

DĒPARTEMENT GĒNIE INFORMATIQUE

Mémoire de fin d'étude pour l'obtention du :

MASTER 2 EN MANAGEMENT DE LA SĒCURITE DES SYSTĒMES D'INFORMATION

SUJET :

MISE EN PLACE D'UN PLAN DE CONTINUITĒ D'ACTIVITĒ EN MILIEU BANCAIRE : CAS DE LA BANQUE ATLANTIQUE TOGO

Présenté par :

Mme DILLE Djamila

Encadrants :

Pr DIALLO Chérif

Pr Khadidiatou Wane Keïta

Maitre de stage :

Mr AFASSI Édouard

Année académique 2019-2020



Un Peuple – Un But – Une Foi

RĒPUBLIQUE DU SENEGAL

UNIVERSITĒ CHEIKH ANTA DIOP DE DAKAR



ĒCOLE SUPĒRIEURE POLYTECHNIQUE

DĒPARTEMENT GĒNIE INFORMATIQUE

Mémoire de fin d'étude pour l'obtention du :

MASTER 2 EN MANAGEMENT DE LA SĒCURITE DES SYSTĒMES D'INFORMATION

SUJET :

MISE EN PLACE D'UN PLAN DE CONTINUITĒ D'ACTIVITĒ EN MILIEU BANCAIRE : CAS DE LA BANQUE ATLANTIQUE TOGO

Présenté par :

Mme DILLE Djamila

Encadrants :

Pr DIALLO Chérif

Pr Khadidiatou Wane Keïta

Maitre de stage :

Mr AFASSI Édouard

Année académique 2019-2020

UNIVERSITĒ CHEIKH ANTA DIOP DE DAKAR



ĒCOLE SUPĒRIEURE POLYTECHNIQUE

DĒPARTEMENT GĒNIE INFORMATIQUE

BP 5085 Dakar-Fann – Téléphone : (221) 33 825 7528 – Fax : (221) 33 825 3724

AUTORISATION DE DEPOT DE MEMOIRE

Je soussigné, Pr Chérif DIALLO

Professeur Assimilé en Informatique, Directeur du Centre de Calcul Ousmane Seck

de l' Université Gaston Berger de Saint – Louis,

En ma qualité d'encadrant de l'étudiante Mme DILLE Djamila

dans le cadre de son stage de fin de cycle du Master 2 en Management de la Sécurité des Systèmes d'Information

Lui donne l'autorisation de déposer son mémoire.

Saint-Louis, le 12 mars 2021

Pr. Chérif DIALLO

REMERCIEMENTS

Tout d'abord, toute la Gloire revient à **Allah SWT** !
C'est par Sa Grâce que j'ai pu accomplir le présent travail.

Je tiens également à remercier chaleureusement mes encadrants :

➔ Professeur Chérif Diallo
➔ Professeur Khadidiatou Wane Keïta
Merci pour votre soutien, vos encouragements, vos conseils, votre engagement et votre disponibilité tout au long de la rédaction de ce Mémoire.

Un grand merci également à mon maitre de stage,

➔ Mr Edouard AFASSI, chef du Service IT de la Banque Atlantique Togo (BATG)
Merci pour l'aide précieuse que vous m'avez apportée durant et après mon stage. Merci aussi pour votre engagement sans faille, pour tous vos conseils et votre dévouement pour la réussite de ce travail.

Merci à Mr Daniel GALADIMA, DG de la BATG, pour m'avoir fait confiance et accordé le stage dans sa structure.
Merci également à toute l'équipe de la BATG pour leur accueil et leur disponibilité sans laquelle ce Mémoire n'aurait pas pu être complété ; mention spéciale à Messieurs Savior, Christian et Donné.

Mes remerciements vont aussi à toute l'équipe de la Bank Of Africa (BOA) Niamey pour m'avoir initié à la Sécurité des systèmes d'information dans le milieu bancaire ; Messieurs BIGA, Moktar, Aboul Aziz, Kader, Madame Fatou.

Je remercie enfin tout le corps enseignant du MSSI ainsi que l'administration du département Génie Informatique pour leurs conseils et leur soutien tout au long la formation.
Merci aussi à tous ceux qui ont contribué de près ou de loin à l'accomplissement de ce travail et que je n'ai pas cité ici.

DĒDICACE

Je dédie ce travail à toute ma famille :

- ➔ Mon regretté père, qui était pour moi un modèle d'intégrité, de fiabilité et de dépassement de soi ; puisses-tu reposer en paix !
- ➔ Ma mère qui n'a cessé de me guider, de m'encourager et de prier pour moi tous les jours. Aucune dédicace ne saurait être assez éloquente pour exprimer ce que tu mérites pour tous les sacrifices que tu n'as cessé de faire depuis ma naissance.
- ➔ Mes frère et sœurs, Aichatou, Bibata, Ouma Kaltoum, Issimouha, Ahmed, Rahamou, Rahila. Vous m'avez toujours soutenu, encouragé à donner le meilleur de moi-même, à persévérer et à toujours garder la foi, et ceci, quelle que soit la situation. Vous m'avez accompagné tout au long de ces années qui n'ont pas été de tout repos !
- ➔ Mon époux, Ibrahim et mes deux adorables filles, Tatiana et Nélia. Vous êtes une inspiration à ne jamais baisser les bras et à toujours aller de l'avant.
- ➔ Mes tantes, oncles, cousins et cousines, mes neveux et nièces.
- ➔ Mes amis, qui sont devenus comme des sœurs et des frères de sang.

Acceptez cette dédicace en témoignage de l'attachement, de l'amour et de l'affection profonde que je vous porte.

Merci infiniment à vous tous !

AVANT PROPOS

L'école Supérieure Polytechnique (ESP) est un établissement public à vocation interafricaine de formation Professionnelle dotée d'une personnalité juridique et d'une autonomie financière. Elle a été créée en 1994 et fait partie intégrante de l'Université Cheikh Anta Diop de Dakar (UCAD). Elle se composait à l'époque du centre de Dakar et du centre polytechnique de Thies.

Elle a pour mission de former, tant sur le plan théorique que pratique des techniciens supérieurs, des ingénieurs technologues, des ingénieurs de conception, des managers en gestion d'entreprise et des docteurs.

L'école dispense des enseignements supérieurs de qualité en vue de préparer aux fonctions d'encadrement dans divers domaines tels que la production, la recherche appliquée et les services.

L'ESP compte 6 départements : Génie Chimique et Biologie Appliquée ; Génie Civil ; Génie Electrique ; Génie Informatique ; Génie Mécanique ; Gestion.

Dans le cadre du Master en Sécurité, les formations enseignent les méthodologies de gestion de la sécurité, avec une approche globale des problèmes, des risques et des solutions, des méthodes pour le traitement de l'information pour la sécurité, des technologies de sécurisation spécifiques, des méthodes et outils de l'enquête numérique pour la lutte contre la cybercriminalité. Elles permettent l'acquisition d'une double compétence en sécurité des systèmes d'information : managériale (gestion de la sécurité, des systèmes) et technologique (réseaux, systèmes, cryptographie).

Après la partie des cours théoriques, les étudiants sont tenus d'effectuer un stage pratique en entreprise afin d'acquérir un savoir-faire, de confronter les connaissances acquises aux réalités professionnelles, et de travailler sur un projet de fin d'études afin de rédiger un Mémoire.

C'est ainsi que nous avons effectué un stage de 2 mois au sein de la BOA puis un autre de 4 mois à la BATG. Durant ces deux périodes, nous avons travaillé sur le sujet suivant : Mise en place d'un plan de continuité d'activité (PCA) dans le domaine bancaire ; cas spécifique de la Banque Atlantique Togo.

RESUMĒ

SUJET DE MÉMOIRE : Mise en place d'un Plan de Continuité d'Activités dans le domaine bancaire : Cas de la Banque Atlantique Togo BATG

Auteure : DILLE DJAMILA – Management de la Sécurité des Systèmes d'Information II

École Supérieure Polytechnique Dakar-Sénégal

La Banque Atlantique est une filiale du Groupe Banque Centrale Populaire (BCP) du Maroc et se présente comme étant le 3ème plus grand groupe bancaire de la zone UEMOA en termes de parts de marché. L'année 1978 voit la création de la Banque Atlantique Côte d'Ivoire, puis en 2006, les filiales du Togo, Niger, Burkina, Mali et Sénégal sont à leur tours créées.

Le réseau informatique et télécom du groupe est bâti autour du centre de production d'Atlantique Technologies à Abidjan, et les filiales s'y connectaient pour la plupart des opérations métier. Ce n'est qu'en 2015, avec des besoins en hausse, que les filiales, dont la Banque Atlantique Togo (BATG), commencent à disposer de serveurs en local et que le besoin de continuité se fait alors ressentir.

Ce document présente les éléments pour la mise en place d'un Plan de continuité d'activité dans le cas où un sinistre grave atteindrait le siège de la BATG.

À cet effet, nous avons identifié les activités et processus essentiels à la continuité de la Banque et les avons évalué et classé par criticité. Nous avons par la suite analysé et cartographié les risques et identifié différents scénarios de crise qui justifient une démarche de continuité. Puis, nous avons procédé à la description des différents plans qui composent le plan de repli global, c'est-à-dire les plans de secours Métier, Informatique et télécom, Logistique et de Gestion de Crise. Nous avons enfin fait des propositions d'emplacements pour y implanter le site de secours et réalisé une évaluation du coût global du projet.

Mots clés : PCA, Site de secours, Banque Atlantique Togo, Analyse de risques, Scénarios de crise, Plan de secours informatique, Plan de gestion de crise.

ABSTRACT

SUBJECT OF THESIS: Establishment of a Business Continuity Plan in the banking sector: Case of Atlantic Bank of Togo ABTG

Author: DILLE DJAMILA - Information Systems Security Management II

École Supérieure Polytechnique Dakar-Senegal

Banque Atlantique is a subsidiary of the Banque Centrale Populaire (BCP) Group from Morocco and presents itself as the 3rd largest banking group in the WAEMU zone in terms of market share. The year 1978 saw the creation of Banque Atlantique Côte d'Ivoire, then in 2006, the subsidiaries of Togo, Niger, Burkina Faso, Mali, and Senegal were created.

The group's IT and telecom network is built around Atlantique Technologies' production center in Abidjan, and the subsidiaries used to connect to it for most of their business operations. It was only in 2015, with the increasing needs, that subsidiaries, including Banque Atlantique Togo (BATG), began to have local servers, and the need to plan for continuity of activity arose.

This document presents the elements for the implementation of a Business Continuity Plan in case a serious disaster affects the headquarters of the BATG.

Therefore, we've identified the activities and processes that were essential to the Bank's business continuity, evaluated and classified them by criticality. Then, we analyzed and mapped the risks and identified different crisis scenarios that would justify a continuity approach. Next, we described the various plans that compose the overall fallback plan, meaning, the Business, IT and Telecom, Logistics and Crisis Management contingency plans.

Finally, we made proposals for locations to establish the backup site and assessed the overall cost of the project.

Keywords: BCP, Emergency site, Banque Atlantique Togo, Risk analysis, Crisis scenarios, IT backup plan, Crisis management plan.

TABLE DES MATIÈRES

RESUMÉ **7**

ABSTRACT **8**

INTRODUCTION GÉNÉRALE **16**

CHAPITRE 1 : ASPECTS NORMATIFS, RÉGLEMENTAIRES ET CYCLE DE VIE DU PCA **18**

1.1. ASPECTS NORMATIFS ET RÉGLEMENTAIRES 18

1.1.1 Règlementation ***18***

1.1.2 Norme ***19***

1.1.3 Cycle de vie du PCA ***20***

1.1.4 Étapes de mise en œuvre ***22***

CHAPITRE 2 : CONTEXTE DE LA BANQUE ATLANTIQUE TOGO (BATG) **25**

2.1. PRÉSENTATION DE LA BANQUE ATLANTIQUE TOGO 27

2.1.1. Agences à Lomé et à l'intérieur du pays ***28***

2.2. PRÉSENTATION DE L'ARCHITECTURE DU SYSTÈME D'INFORMATION DE LA BATG 28

2.2.1. Description des « réseau, exploitation et infrastructures » de la BATG ***28***

2.2.2. Schéma de l'architecture du réseau de la BATG ***30***

2.2.3. Site de secours existant ***31***

CHAPITRE 3 : PCA POUR LA BATG **34**

3.1. DÉFINITION DU PÉRIMÈTRE ET DES BESOINS EN CONTINUITÉ D'ACTIVITÉ 34

3.1.1. Énumération des activités par service ***34***

3.1.2. Identification et management des processus métiers et impacts financiers de leur arrêt ***41***

3.1.3. Analyse des Risques et Cartographie pour les activités et les processus critiques ***51***

3.1.3.1. Procédure d'analyse de risques ***51***

3.1.3.2. Cartographie des risques ***52***

3.2. IDENTIFICATION ET FORMALISATION DES BESOINS EN CONTINUITÉ D'ACTIVITÉ 57

3.2.1. Stratégie de continuité ***57***

3.2.2. Besoins de continuité pour les ressources critiques ***62***

3.3. ARCHITECTURE RÉSEAU TYPE A METTRE EN ŒUVRE DANS LE CADRE DU PCA D'UNE FILIALE DU GROUPE ABI 72

3.3.1. En situation normale..... 72

3.3.2. En mode PCA..... 73

3.3.3. Cas de BATG..... 74

3.3.3.1. En situation normale..... 74

3.3.3.2. En mode PCA..... 75

3.4. CHOIX DU SITE DE REPLI 76

3.4.1. Conditions d'implantation..... 76

3.4.2. Propositions de sites..... 80

3.4.2.1. Proposition 1 : 80

3.4.2.2. Proposition 2 : 82

3.4.2.3. Analyse de risques des propositions..... 85

CHAPITRE 4 : DÉFINITION DES SOLUTIONS DE SECOURS..... 89

4.1. PLAN DE REPLI ET LOGISTIQUE 89

4.2. PLAN DE SECOURS MÉTIERS 89

4.2.1. Besoins pour le secours métiers 89

4.2.2. Secours agences..... 90

4.3. PLAN DE SECOURS INFORMATIQUE ET TÉLÉCOM (PSI) 90

4.3.1. Description de la Cellule de Crise Informatique (CCI)..... 91

4.3.2. Phases du PSI..... 91

4.3.2.1. Phase 1 : Réponse d'urgence au sinistre..... 92

4.3.2.2. Phase 2 : Mobilisation de l'équipe de restauration du volet IT..... 92

4.3.2.3. Phase 3 : Restitution du Système d'information, des applications et des données..... 93

4.3.2.4. Phase 4 : Mise en service des outils et validation de l'intégrité du système et des données..... 93

4.3.2.5. Phase 5 : Restauration et recréation des données et transactions perdues..... 93

4.3.2.6. Phase 6 : Restauration des fonctions du métier..... 94

4.3.2.7. Besoins métiers à secourir..... 94

4.3.2.8. Restauration réseaux et Télécom..... 96

4.4. GESTION DE LA CRISE 96

4.4.1. Le Responsable du Plan de Continuité d'Activité (RPCA) 97

4.4.2. Les correspondants du Plan de Continuité d'Activité (CPCA) 97

4.4.3. Définition des cellules de crise..... 98

4.4.3.1. La Cellule de Crise Décisionnelle (CCD)..... 98

4.4.3.2. La cellule des Remontées des Incidents Majeurs (CRIM)..... 99

4.4.3.3. La Cellule de Crise Métier (CCM) 100

4.4.3.4. La Cellule de Crise Informatique (CCI) 100

4.4.3.5. La Cellule de Crise Ressources Humaines et Logistiques (CCRHL) 101

4.4.3.6. La Cellule de Communication de Crise (CCC)..... 101

4.4.3.7. Maintien en condition opérationnelle du PCA..... 104

4.5. PROCESSUS PCA : LOGIGRAMME..... 105

CHAPITRE 5 : ÊVALUATION DU COUT DU PROJET..... 106

5.1. SITUATION GÊOGRAPHIQUE DU SITE RETENU..... 106

5.2. ÊVALUATION DU COUT DES INFRASTRUCTURES 108

5.2.1. Construction de l'immeuble 108

5.2.2. Équipements..... 110

5.2.3. Coût total..... 111

CONCLUSION GÊNÊRALE 112

RÊFÊRENCES 114

TABLE DES FIGURES

Figure 1 : Circulaires No 01-2017 et No 04-2017 de la BCEAO. 18
Figure 2 : PLAN-DO-ACT-CHECK. 21
Figure 3 : Cycle de vie du PCA. 22
Figure 4 : Organigramme d'ABI. 26
Figure 5: Schéma de l'architecture du réseau de la BATG. 30
Figure 6 : Exemple d'un processus métier : PROCESSUS VIREMENT. 44
Figure 7 : Pourcentage par département dans les processus critiques. 47
Figure 8 : Schéma d'architecture type du groupe ABI. 72
Figure 9 : Schéma d'architecture de la BATG. 74
Figure 10 : Schéma d'architecture type pour BATG en mode PCA. 75
Figure 11 : Proposition Site de KOVIE. 80
Figure 12 : Proposition site d'AVETA. 81
Figure 13 : Proposition site de NOEPE. 81
Figure 14 : Site de Sanguera. 83
Figure 15 : Site de Sanguera, Satellite. 83
Figure 16 : Site de Sanguera, distances. 84
Figure 17 : Phases du PSI. 92
Figure 18 : Membres de la CCD. 99
Figure 19 : Membres de la CRIM. 99
Figure 20 : Membres de CCM. 100
Figure 21 : Membres de la CCI. 100
Figure 22 : Membres de la CCRHL. 101
Figure 23 : Membres de la CCC. 102
Figure 24 : Logigramme processus PCA. 105
Figure 25 : Position site de repli de NOEPE. 106
Figure 26 : Site de NOEPE, routes. 107
Figure 27 : Site de NOEPE, Satellite. 107
Figure 28 : Site de NOEPE Coordonnées. 108

TABLE DES TABLEAUX

Tableau 1 : Aménagement du site de repli existant. 31

Tableau 2 : Activités majeures par service. 36

Tableau 3 : Processus essentiels par département. 42

Tableau 4: Interventions par département dans les processus critiques de la banque. 45

Tableau 5: Pondération par service. 46

Tableau 6: Impacts de l'arrêt des activités essentielles. 48

Tableau 7 : Probabilité et Impact. 52

Tableau 8 : Synthèse = Probabilité X Impact. 52

Tableau 9: Niveau de risque. 53

Tableau 10: Cartographie des risques pour la BATG. 54

Tableau 11 : Besoins par service. 58

Tableau 12: Effectifs en ressources humaines à secourir et nombre de machines associées. 62

Tableau 13 : DMIA pour les services critiques et besoins secours métiers. 63

Tableau 14 : Effectifs du site de Repli. 78

Tableau 15 : Cartographie Risques des propositions de site de repli. 85

Tableau 16: Besoins Métier à secourir. 95

Tableau 17 : Personnes critiques et leur backup. 102

Tableau 18 : Proposition de construction d'une nouvelle agence. 109

Tableau 19 : Estimation du cout de la construction du site secours. 109

Tableau 20: Devis estimatif de la sécurité de la salle technique du site de secours et des liaisons filaires. 110

Tableau 21 : Coût final du site de secours. 111

ABRĒVIATIONS

ABI : ATLANTIC BUSINESS INTERNATIONAL

BATG : BANQUE ATLANTIQUE TOGO

BCEAO : Banque Centrale des États de l'Afrique de l'Ouest

BLR : Boucle Locale Radio

BOA : BANQUE OF AFRICA

CCC : Cellule de Communication de Crise

CCD : Cellule de Crise Décisionnelle

CCI : Cellule de Crise Informatique

CCM : Cellule de Crise « Métier »

CCRHL : Cellule de Crise Ressources Humaines et Logistique

CPCA : Correspondant du PCA

DAI : DIRECTION de l'AUDIT INTERNE

DBD : DIRECTION BANQUE DE DĒTAIL

DBE : DIRECTION BANQUE DE L'ENTREPRISE

DE : DIRECTION des ENGAGEMENTS

DFC : DIRECTION FINANCE et COMPTABILITĒ

DJG : DIRECTION JURIDIQUE et GOUVERNANCE

DMIA : Durée maximale d'interruption admissible

DO : DIRECTION des OPÉRATIONS

DRC : DIRECTION RISQUE et CONTRÔLE

DRH : DIRECTION des RESSOURCES HUMAINES

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ISO : International Standard Organization

IT : INFORMATION TECHNOLOGY

OIV : Opérateurs d'Importance Vitale

PCA : PLAN DE CONTINUITĒ D'ACTIVITĒ

RPCA : Responsable du PCA

SI : Système d'Information

SLI : SERVICE LOGISTIQUE et IMMOBILISATION

UEMOA : Union Economique et Monétaire Ouest Africaine

VPN : Virtual Private Network

VSAT : Very Small Aperture Terminal

WAEMU: West African Economic and Monetary Union

INTRODUCTION GĒNĒRALE

Catastrophes naturelles, actes de malveillance, évènements imprévus, politiques, pannes matérielles et logicielles lourdes, cybercriminalité, et une panoplie d'autres risques sont des préjudices de plus en plus fréquents et couteux auxquels sont exposés de nos jours, les entreprises. Ces différents risques sont malheureusement accompagnés de conséquences majeures qui paralysent leurs activités ou leur fonctionnement.

L'image de marque et la confiance des clients étant des notions essentielles dans de nombreux secteurs, notamment ceux relatifs aux services, beaucoup d'entreprises ne survivent pas à un arrêt complet de leurs activités d'une durée de plus de 3 jours.

Un proverbe chinois dit : « les tuiles qui protègent de la pluie ont toutes été posées par beau temps » ; et un autre plus courant reprend : « Il vaut mieux prévenir que guérir » ; car lorsqu'un sinistre arrive, il est déjà trop tard pour mettre en œuvre un plan ! Bien qu'il soit utopique de chercher à tout prévoir et maîtriser, le responsable d'une entreprise ou d'une organisation – publique ou privée – se doit de concevoir et de mettre en œuvre des stratégies de protection permettant d'éviter certains événements, ou du moins d'en limiter les effets directs sur les objectifs de l'entreprise et d'assurer la continuité de l'activité malgré la perte de ressources critiques.

Un Plan de Continuité d'Activités **(PCA)** a par conséquent pour objet de décliner la stratégie et l'ensemble des dispositions qui sont prévues pour garantir à une entreprise, la reprise et la continuité de ses activités à la suite d'un sinistre ou d'un événement perturbant gravement son fonctionnement normal. Il doit permettre à l'entreprise de répondre à ses obligations externes (législatives ou réglementaires, contractuelles) ou internes (risque de perte de marché, survie de l'entreprise, image…) et de tenir ses objectifs. C'est un projet transversal qui prend en compte globalement toutes les activités et processus de l'entreprise. [1]

Une fois élaboré, le PCA regroupe les procédures documentées qui vont servir de guide à l'entreprise afin de lui permettre de répondre, rétablir, reprendre et retrouver un niveau de fonctionnement prédéfini à la suite d'une perturbation importante, la rendant ainsi plus résiliente dans un monde de risques.

C'est dans cette logique que la BATG, depuis 2016, vu la taille et la criticité de son infrastructure grandissante ces dernières années, a initié le projet de mise en place d'un site de secours pour assurer la continuité de son activité. Cependant, ce site de secours est toujours dans un état provisoire faute d'espace adéquat. C'est dans ce contexte qu'il nous a été confié lors de notre stage à la banque, le projet de déterminer un nouveau

site de repli définitif et de proposer les éléments d'une opérationnalisation répondant aux exigences et standards internationaux.

L'objectif de la présente étude va ainsi plus largement consister en l'élaboration d'un PCA global au niveau du siège de la Banque Atlantique Togo (BATG) ; de l'expression des besoins et la formalisation des objectifs de continuité selon la stratégie définie par la direction en passant par l'analyse des risques retenus comme les plus graves pour la continuité, et la définition des solutions de secours, puis le dispositif de gestion de crise, ainsi que les coûts du site PCA.

Notre travail va donc s'articuler autour 3 grands axes :

1. Une introduction pour présenter et décrire, l'État de l'Art du PCA
2. Une présentation de la BATG avec étude de l'existant
3. La définition des différentes étapes de mise en œuvre du PCA et l'évaluation du coût du projet.

CHAPITRE 1 : ASPECTS NORMATIFS, RĒGLEMENTAIRES ET CYCLE DE VIE DU PCA

1.1. ASPECTS NORMATIFS ET RĒGLEMENTAIRES

1.1.1 Règlementation

Les risques, dans le domaine bancaire ces dernières années, sont en hausse vertigineuse, vu la recrudescence des cyber-attaques et autres fraudes en tous genre !

Dans le monde en général, et particulièrement en France, les banques font partie des opérateurs d'importance vitale (**OIV**) qui ont l'obligation légale de prévoir des PCA. Cette obligation française, précisée par l'arrêté du 3 novembre 2014 est relative au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumis au contrôle de l'ACPR (Autorité de contrôle prudentiel et de résolution), texte qui remplace le Règlement CRBF 97-02 (Le règlement du Comité de la Réglementation Bancaire et Financière n°« 97-02 » vise à doter les établissements de crédit d'un ensemble de systèmes de mesure, de maîtrise et de contrôle de leurs risques). [2]

Les sanctions civiles qu'encourt un employeur qui enfreint la réglementation sont ainsi celles sanctionnant la faute injustifiable à raison de la réalisation d'un risque survenu en l'absence d'évaluation préalable du risque et de mise en œuvre de mesures de protection.

En Afrique de l'Ouest, bien que pouvant relever du choix personnel de l'entreprise, le PCA est nécessaire d'un point de vue réglementaire pour les établissements financiers [3]. Il est exigé selon la règlementation bancaire dans l'espace UEMOA. Les circulaires de la Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) sont présentées sur la figure 1 :

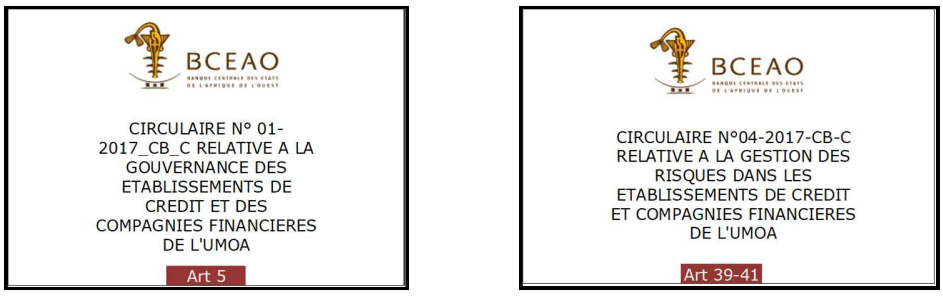


Figure 1 : Circulaires No 01-2017 et No 04-2017 de la BCEAO.

1.1.2 Norme

Le management de la continuité d'activité est soumis à la norme : ISO 22301 qui « spécifie la structure et les exigences relatives à la mise en œuvre et à la maintenance d'un Système de Management de la Continuité d'Activité (SMCA) qui développe une continuité d'activité en fonction de l'importance et du type d'impact que l'organisme peut ou non accepter suite à une perturbation ». [4]

Un PCA est donc nécessairement évolutif car les priorités de l'organisme évoluent avec les modifications d'objectifs, d'obligations contractuelles ou réglementaires, de relations avec des partenaires externes (fournisseurs ou clients) et d'appréciation du risque. Il doit être revu régulièrement pour tenir compte de l'évolution de ces paramètres.

Toute personne en charge d'une action relevant du PCA doit connaître précisément son rôle et ce qu'elle doit faire concrètement en cas de sinistre. Ainsi, la documentation du PCA doit faciliter l'adhésion des personnes concernées, l'adaptabilité des mesures à la situation et l'évolutivité du plan dans le temps, en incluant une description du contexte, des scénarios de risque retenus et de la stratégie de réponse.

Par conséquent, la recommandation est que le PCA comprenne les phases suivantes qui doivent être élaborées successivement [1] :

- ➔ Le contexte : l'expression des besoins en continuité d'activité (EBCA) afin de pouvoir délimiter un périmètre. Il faut énumérer et formaliser tous les processus métiers internes ou externes afin d'identifier ceux nécessaires au fonctionnement des activités essentielles. Il faut aussi inclure dans l'analyse, les échanges avec les prestataires ou les fournisseurs. Un incident chez un partenaire ou un fournisseur peut en effet avoir des conséquences importantes sur l'activité. Cette étape, aussi appelée BIA=Business Impact Analysis, doit être faite avec chaque responsable de service.

- ➔ L'analyse de risques et la notion d'acceptabilité : les risques retenus comme les plus graves pour la continuité d'activité doivent être clairement explicités au moyen de scénarios. Il est fortement recommandé de conduire une analyse complète des risques, de façon à disposer d'une grille d'évaluation et de critères objectifs pour décider des priorités.

  Il est possible par exemple d'imaginer tous les types de scénarios, même ceux qui peuvent paraitre rarissimes ou peu probables (comme une crue, un tremblement de terre, une attaque terroriste, une pandémie, une guerre, la destruction d'un site…) focalisés sur les conséquences sans forcément en décrire les causes ; cela peut suffire à élaborer une première version de PCA simplifié.

➔ La stratégie de continuité d'activité : elle doit être établie et décrite en précisant, pour chaque activité essentielle, les niveaux de service retenus et les durées d'interruption maximales admissibles pour ces différents niveaux de service, ainsi que les ressources et procédures permettant d'atteindre les objectifs, en tenant compte des ressources critiques qui peuvent avoir été perdues, jusqu'à la reprise de la situation normale.

➔ Le dispositif de gestion de crise : Il consiste en l'organisation de la cellule de crise qui permet de conduire la mise en œuvre du PCA en assurant le pilotage des actions de réponse et de gestion de l'incertitude, à travers les procédures de détection d'incident, de qualification, d'escalade, d'alerte, de mobilisation, d'activation de la cellule de crise, d'anticipation, d'intervention, de déclenchement des dispositions du PCA (solution palliative, mode secours avec fonctionnement dégradé) et de communication (primordiale, en externe ou interne afin d'éviter toute dissonance et donner une impression générale de maitrise des évènements).

➔ Les tests et le maintien en fonction opérationnelle du PCA. Cette action essentielle consiste en premier lieu à établir des indicateurs permettant de vérifier et mesurer la bonne mise en œuvre des dispositifs préconisés dans le plan ainsi que l'efficacité du plan au regard des objectifs de continuité.
Durant une crise, on vérifiera les niveaux de service constatés sur les activités essentielles, le fonctionnement des processus spécifiques au PCA et la disponibilité des ressources de secours.
La maintenance opérationnelle consiste ensuite à mettre en place les dispositifs de mesure relatifs à des tests périodiques, à des exercices ou à un sinistre vécu. Les axes de progrès doivent être identifiés et le suivi des améliorations apportées au plan.

1.1.3 Cycle de vie du PCA

La norme ISO 22301 [4] (management de la continuité d'activité) est orientée processus et propose en toute logique une démarche d'amélioration continue à 4 phases (Figure 2) :
Plan= Planifier ; Do= Dérouler ; Check= Contrôler ; Act= Agir.

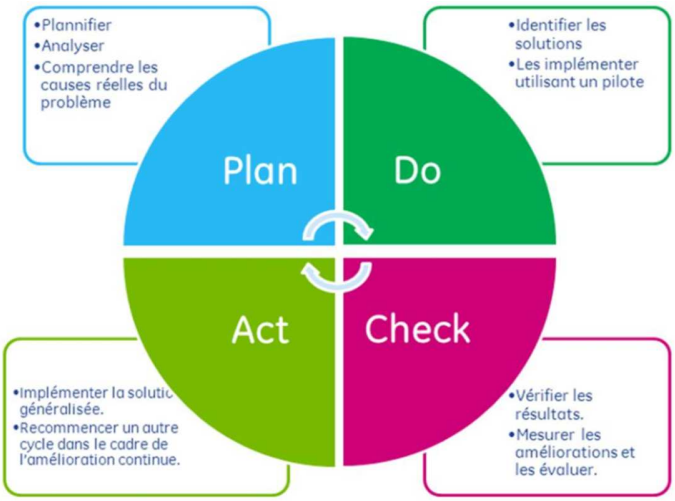


Figure 2 : PLAN-DO-ACT-CHECK.

La démarche adopte une spirale évolutive régulière : la fin d'un cycle entraîne le début d'un nouveau, comme dans la roue de Deming (modèle PDCA) ci-dessus ; Ce concept est largement connu dans le domaine de la qualité.

➔ L'étape de la **planification** identifie les mesures à prendre dans l'organisation (Périmètre et Politique), mais ne permet pas de les mettre en place concrètement. Il faut les organiser, sélectionner les moyens nécessaires et définir les responsabilités en établissant un plan de traitement des risques.

➔ L'étape du **déroulement** utilise de nombreux moyens techniques pour la mise en œuvre. Il convient de choisir les moyens nécessaires, suffisants, et adéquats. Il convient aussi de sensibiliser et de former l'ensemble du personnel pour qu'ils adoptent et intègrent dans leur vie de tous les jours, des comportements préventifs de crises.

➔ L'étape du **contrôle** se donne des moyens de surveiller l'efficacité du PCA ainsi que sa conformité. Des indicateurs seront définis pour vérifier la bonne mise en œuvre des dispositifs. Le plan doit être revu et mis à jour régulièrement. Des simulations de crise doivent aussi être effectuées.

➔ L'étape de **l'action** analyse et met en place des démarches pour agir sur les effets et corriger le plan après la mise en lumière de dysfonctionnements grâce à la phase du contrôle. On agit aussi sur les causes pour éviter que l'incident ne se reproduise, dans un but d'amélioration continue.

1.1.4 Étapes de mise en œuvre

La mise en place et le maintien du PCA se réalisent en six étapes successives (Figure 3). Ces six étapes sont plus ou moins difficiles à mettre en œuvre, car elles nécessitent à chaque fois la participation de plusieurs intervenants ainsi que la validation de la direction.

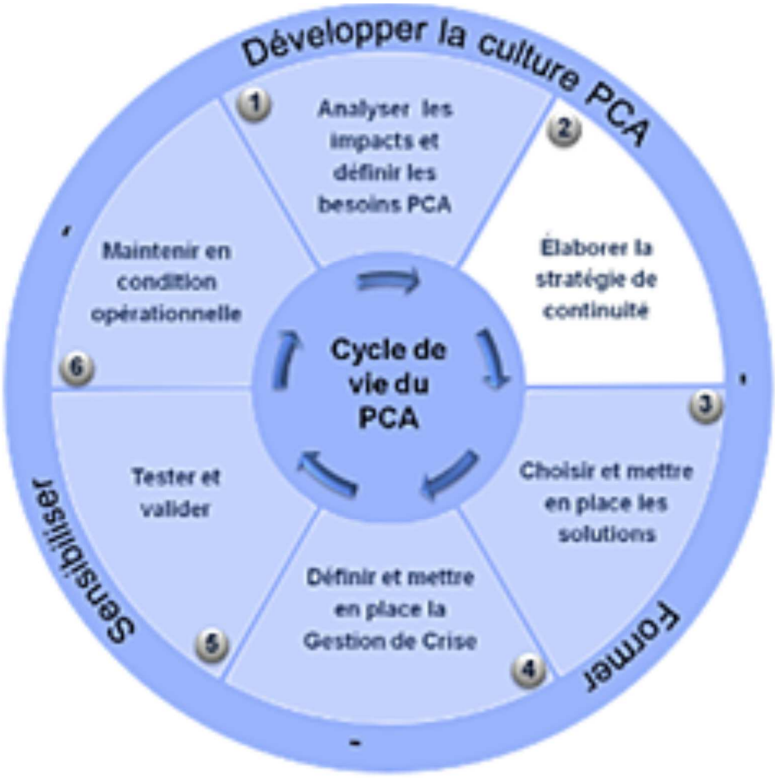


Figure 3 : Cycle de vie du PCA.

➔ Définir les besoins en continuité d'activité [1].

Cette première action est essentielle et conditionne l'efficacité d'ensemble de la démarche. Elle vise à préciser le périmètre géographique et fonctionnel de l'organisation qui doit être pris en compte, puis à identifier tout ce qui peut orienter les choix en rapport avec la spécificité de l'organisation. Il faut préciser, pour chaque activité essentielle et chaque processus ou flux critique, le niveau de service minimum indispensable ainsi que la durée d'indisponibilité maximale acceptable. Pour maintenir ou rétablir le fonctionnement des processus, il faut disposer de ressources dites « critiques » que l'on peut classer en cinq catégories : ressources humaines, infrastructures, système d'information, ressources intellectuelles, et fournisseurs externes. Pour simplifier, l'analyse des besoins en ressources peut être effectuée sur la base d'un nombre limité de scénarios ou situations de crise retenue comme prioritaires, à l'issue de la démarche de gestion de risque et compte tenu des besoins de continuité. Cette démarche analytique est nécessaire pour la suite, afin de

permettre d'apprécier le niveau de risque acceptable par l'organisation, et d'orienter en conséquence la stratégie de continuité, soit vers une approche privilégiant la continuité des activités principales, soit, au contraire, vers une approche acceptant plus facilement les pertes d'activité associées à la prise de risque. L'analyse du contexte permet également d'identifier les activités qui sont essentielles pour l'atteinte des objectifs de l'organisation et le respect de ses obligations.

➔ Élaborer la stratégie de continuité.

Lorsque les moyens à mettre en œuvre pour assurer la continuité ou la reprise d'activité ont été identifiés, leur coût peut être évalué. Celui-ci est d'autant plus élevé que les objectifs de délais d'interruption sont courts. Il est par conséquent possible de déterminer le point d'optimisation, en prenant en compte la probabilité d'occurrence du scénario de crise et l'appétence ou aversion au risque de l'organisation, pour l'activité considérée. En pratique, ces calculs financiers peuvent être parfois très complexes. Dans ce cas l'ordre de grandeur quantitatif et qualitatif des coûts justifiant la mise en place d'une stratégie de continuité peut être estimé afin d'obtenir une validation en connaissance de cause par la direction.

➔ Choisir et mettre en place les solutions.

Après avoir défini les besoins ainsi que la stratégie de continuité d'activité, il est à présent possible de rédiger le plan de continuité d'activité qui va décrire la démarche logique ayant conduit au choix de la stratégie et de la réponse aux différents scénarios de crise retenus. Cette réponse consiste à préciser les moyens et à documenter les procédures qu'il convient de mettre en œuvre en fonction des dispositifs du PCA. Les responsables de ces moyens et procédures doivent être clairement identifiés ainsi que leur rôle et les actions attendues d'eux. La documentation doit être facilement accessible en cas de besoin et être aisément comprise même par des personnes récemment affectées et qui n'ont pas encore été formées.

➔ Définir et mettre en place la gestion de crise.

La gestion de crise, entendue au sens large, conduit à mettre en œuvre les dispositifs et procédures nécessaires pour détecter, qualifier, alerter, anticiper, conduire les actions utiles, et décider notamment de l'activation de certains dispositifs du PCA. Dans cette perspective, les fonctions clés de la gestion de crise sont : la veille, qui permet de détecter des signes précurseurs et donc de préparer les responsables concernés, la procédure d'escalade, qui permet d'alerter les responsables du PCA et de la gestion de crise afin de qualifier l'événement assez tôt pour déclencher l'alerte de la hiérarchie, puis prendre au bon moment la décision d'activer la cellule de crise,

les fonctions d'aide à la décision et notamment la capacité à anticiper, analyser les différents scénarios possibles et recommander un plan d'action optimal dans le contexte incertain inhérent aux situations de crise sortant d'un cadre prédéfini. La capacité de mise en œuvre du plan doit être assurée par les responsables en charge. Ils doivent vérifier la disponibilité des ressources spécifiques conditionnant l'activation du plan de continuité. À défaut, de nouvelles ressources doivent être mobilisées pour assurer cette disponibilité dans les délais prescrits par le PCA. Les procédures de mise en œuvre du PCA doivent également être spécifiées, documentées et intégrées dans les processus existants. Il est nécessaire de vérifier que ces ressources sont bien disponibles ou le seront à une date identifiée, et que les procédures sont connues, comprises et pourront être mises en œuvre dans les délais prescrits, et selon des modalités spécifiques aux scénarios retenus.

➔ Tester, valider.

Il faut faire évoluer le plan par le moyen d'exercices et de retours d'expérience. Il est possible de tester la mise en œuvre des dispositifs par une simulation. Il peut s'agir par exemple du basculement de certaines fonctions sur un site de secours, etc. Les tests doivent être réalisés au moins une fois par an.

➔ Maintenir en condition opérationnelle le PCA.

Une fois le PCA réalisé et sa capacité à être mis en œuvre garantie, il est nécessaire d'en vérifier l'efficacité. À cet effet, différentes approches complémentaires sont recommandées. Il peut s'agir d'abord de faire vérifier les documents, idéalement par un tiers de confiance, de vérifier aussi, par des exercices, que les dispositifs et procédures de continuité sont connus, compris et peuvent être mis en œuvre dans les délais prescrits.

En résumé, le plan de continuité d'activités est une entité normée dont la mise en place et le maintien se fait en plusieurs étapes bien déterminées. Il n'est cependant pas figé et doit être testé et faire l'objet de révisons régulières pour s'adapter aux besoins changeants de l'entreprise.

Nous allons dans la prochaine section, l'étudier dans le contexte particulier de la BATG et analyser ce qui y existe déjà.

CHAPITRE 2 : CONTEXTE DE LA BANQUE ATLANTIQUE TOGO (BATG)

La Banque Atlantique est une filiale du Groupe Banque Centrale Populaire (BCP) du Maroc et est le 3ème plus grand groupe bancaire de la zone UEMOA en termes de parts de marché. Depuis la création de la première entité au début des années 80, le Groupe Banque Atlantique a enregistré de nombreux faits marquants ayant conduit à sa configuration actuelle. Le milieu des années 2000 a été la phase de développement accéléré avec l'implantation dans les différents pays de la zone. Le Groupe a entamé depuis 2009, une phase de consolidation, d'optimisation de ses implantations, et surtout d'ouverture à des partenaires financiers, afin de se doter des moyens nécessaires à l'accompagnement du développement de ses différentes entités. L'année 1978 voit la création de la Banque Atlantique Cote d'Ivoire. Puis en 2006, les filiales du Togo, Niger, Burkina, Mali et Sénégal sont à leur tour créées.

La Banque Atlantique est présente dans huit pays de l'espace UEMOA :

- Bénin.
- Burkina Faso.
- Côte d'Ivoire.
- Guinée-Bissau.
- Mali.
- Niger.
- Sénégal.
- Togo.

La Banque s'appuie également sur des filiales spécialisées telles que les assurances (Atlantique Assurances et Atlantique Assurance Vie en Côte d'Ivoire, GTAC2A IARDT et GTA-C2A Vie au Togo), les banques d'affaires (Atlantique Finance), la gestion d'actifs (Atlantic Asset Management).

Le Groupe BCP est un groupe financier mutualiste et universel qui tire sa force de la singularité de ses valeurs de solidarité et de mutualité marquées dans son organisation et de son fonctionnement unique au Maroc. Sa mission : « Développer le continent par l'inclusion financière ».

Cotée en Bourse depuis le 8 juillet 2004, la BCP agit notamment en qualité de compensateur central du Groupe, gère les excédents de trésorerie des Banques

Populaires Régionales et assure le refinancement ainsi que la gestion des services d'intérêt commun pour le compte des organismes de la Banque.

Après l'ouverture d'une dernière succursale en Guinée Bissau en 2016, le groupe est présent dans 12 pays Africains et dans 13 autres pays dans le reste du monde.
Il fonde son efficacité sur 1600 collaborateurs répartis dans 14 filiales actives dans les domaines de la Banque d'Affaires, de la Banque et des Assurances pour proposer des conseils en matière de financements et des solutions d'investissements en s'appuyant sur l'expertise et le savoir-faire de ses équipes.

Depuis 2012, un partenariat stratégique entre Atlantic Financial Group et le Groupe BCP a donné naissance à **Atlantic Business International** (**ABI**) qui est une holding financière de contrôle et de développement. Cette entité supervise et coordonne les activités des 8 banques opérant dans 8 États de l'UEMOA. Elle se positionne ainsi comme un groupe financier de premier ordre de la région dont le siège se trouve à Abidjan. Son capital est majoritairement (70%) détenu par la BCP du Maroc. L'Organigramme d'ABI est représenté dans la figure 4 :

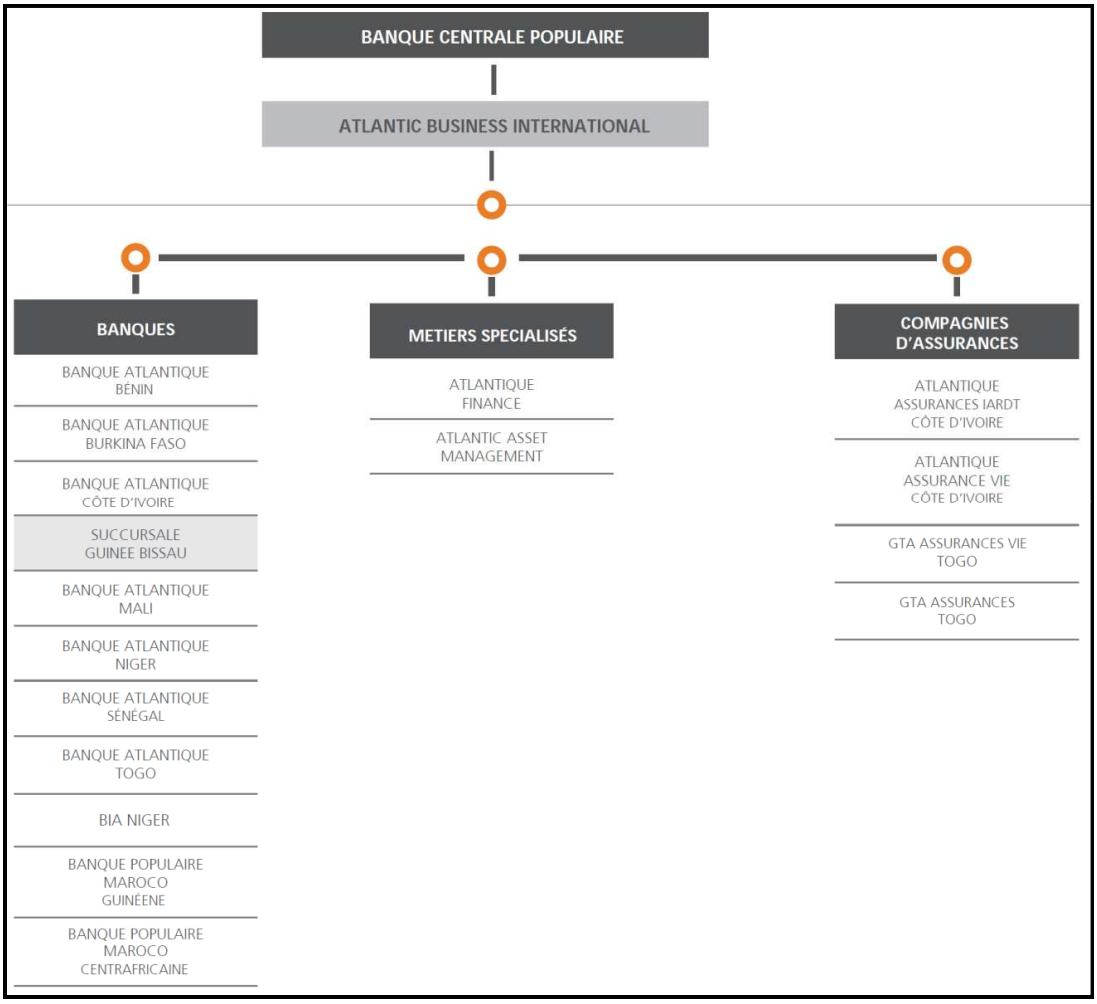


Figure 4 : Organigramme d'ABI.

Pour ABI, il est essentiel que ses filiales soient capables de résilience face à une crise grave. Elles doivent être capables de continuer à satisfaire leurs engagements vis-à-vis des clients, des partenaires ainsi que du législateur et du régulateur même en cas de crise majeure ou de désastre, quitte à ce que ce soit en mode dégradé.

Conformément aux dispositions de Bale II [5], les filiales sont inscrites dans une démarche de maitrise des risques opérationnels. Cette démarche prévoit de mettre en place et d'améliorer les dispositifs de gestion de risques. Il est donc nécessaire de mettre en œuvre des stratégies de protection permettant de limiter les effets directs de certains évènements sur les objectifs de la filiale et d'assurer ainsi la continuité d'activité malgré une perte de certaines ressources. Le dispositif actuel doit par conséquent être renforcé avec la mise en place d'un PCA opérationnel incluant la sélection d'un site de repli adéquat.

Ce site devra répondre à un besoin d'accueil des ressources humaines, matérielles ou logicielles nécessaires à la reprise de l'activité de la filiale en cas d'indisponibilité totale ou partielle de son siège.

Un travail préalable au niveau du Groupe a déjà été fait en 2010 pour la mise en place d'un PCA pour les cas où les Hub d'Abidjan et de Cotonou (qui sont les sites de production et son backup) deviendraient indisponibles, au moment des troubles politiques en Côte d'Ivoire. Depuis lors, les mises à jour du PCA sont faites chaque année.

Tous les serveurs, dans un premier temps, étaient concentrés à Abidjan. Les filiales s'y connectaient pour la plupart des opérations métier. Ce n'est qu'en 2015, avec des besoins en hausse, que les filiales, dont la BATG, ont commencé à disposer de serveurs en local et que le besoin de continuité se fit alors ressentir.

2.1. PRĒSENTATION DE LA BANQUE ATLANTIQUE TOGO

La banque Atlantique Togo a été créée en Avril 2006 à Lomé. Ella a démarré avec un capital de 1 milliard 500 millions de FCFA.

En 2017, le total de ses actifs a progressé de 7,5% pour s'établir à 256 milliards de FCFA. En 2018, elle s'est stabilisée à la 4ème place des banques du Togo avec 8% de part de marché.

La banque propose une large gamme de produits et de services. On compte entre autres : l'épargne, le placement, le compte à vue, le crédit, la monétique, les produits VISA, le transfert d'argent avec MOOV (Flooz), la Bancassurance, les moyens de paiement (Transferts en XOF et en devises, chèques certifiés, chèques de banque), les transferts rapides (Western Union, RIA, Money cash, appels de fonds, etc.), les cartes privatives,

les cartes internationales, le ramassage de fonds, les guichets automatiques, la collecte et gestion des effets, la banque par internet, le SMS Banking, etc.

En Avril 2018, la BATG change d'identité visuelle comme ses filiales sœurs du réseau des Banques Atlantique de l'Afrique de l'Ouest. L'emblème qui était alors un « a » est à présent un cheval en marche.

2.1.1. Agences à Lomé et à l'intérieur du pays

Le réseau de la banque Atlantique Togo est composé de 16 agences à Lomé et de 7 agences à l'intérieur du pays.

Parmi les agences à Lomé il faut citer : Le SIEGE (Place du petit marché, Rue Koukmor), ADIDOGOME, AGOE, AHADJI–KPOTA, ASSIGANTO, BE, HEDZRANAWOE, BAGUIDA, DECKON, IMMEUBLE TABA, ECOMARINE, SOTED, ASSIGAME, TOTI, GTA puis EL SHADAI ATIKOUME qui est un guichet automatique.

La BATG compte aussi 7 agences à l'intérieur du pays dans 7 villes principales du Togo. Il s'agit de : ANIE, ATAKPAME, CINKASSE, DAPAONG, KARA, TABLIGBO, SOKODE. Deux nouvelles agences sont en construction à Lomé afin de répondre à la croissance des activités et aux besoins grandissant des clients de la banque.

2.2. PRĒSENTATION DE L'ARCHITECTURE DU SYSTĒME D'INFORMATION DE LA BATG

Le réseau informatique et télécom du groupe est bâti autour du centre de production d'ATLANTIQUE TECHNOLOGIES à ABIDJAN. Il concentre un ensemble d'applications centralisées (WORC, RTGS, e-BANKING, etc.) sur des serveurs et équipements télécoms dans les sièges de ses filiales.

Le Bénin constitue le centre de secours du réseau du groupe. Il est utilisé en cas d'indisponibilité du centre principal (DATACENTER) d'ABIDJAN.

2.2.1. Description des « réseau, exploitation et infrastructures » de la BATG

Le cœur du réseau de la BATG est centré autour deux Firewalls montés en cluster (HA). Plusieurs domaines virtuels (VDOM) y sont configurés pour renforcer la sécurité de l'infrastructure. Parmi eux, on compte (Figure 5) :

➔ VDOM FILIALES (VD_FILIALE) pour la gestion des réseaux logiques du siège et des agences.

Le Réseau du siège est subdivisé en plusieurs VLANs, une pour chaque département/direction (V_IT pour l'Informatique, V_MONET pour la Monétique, V_OP pour la direction des Opérations, V_DBD pour la direction Banque de Détail, V_DG pour la direction Générale, V_DFC pour la direction Financière et Comptable, V_DRH pour les ressources humaines, etc.).

➔ L'agence principale est reliée au siège (AGP). Tout comme les autres, pour répondre aux exigences de PCI-DSS, elle est subdivisée en plusieurs VLANs. Ainsi dans les agences, chaque entité a son propre VLAN (V_CAISSE pour les caisses, V_CLIENT pour la clientèle, V_DAB pour les guichets automatiques, V_MGMT pour les administrateurs, V_PHONE pour les téléphone fixes, V_PRINT pour les imprimantes, V_MISSION pour les agents en mission ponctuelles).

➔ Des interfaces sont réservées pour les VLANs serveurs. On compte différents types de serveurs :

- Des serveurs système (Contrôleurs de domaine, antivirus, serveur de partage de fichiers, DNS…etc.).
- Des serveurs avec la BCEAO.
- Des serveurs d'applications (Nagios, WORC, Gestion des prêts, Gestion des utilisateurs gesha…etc.).

➔ VDOM INTERNET, pour gérer les liaisons vers Internet (VD_INT).

➔ VDOM PARTENAIRE (VD_PART), pour gérer les partenaires comme la BCEAO.

➔ VDOM DATA pour gérer la relation avec les Datacenter d'Abidjan et de Casablanca (VD_DATA), qui abrite les applications métiers.

- Les centres de productions sont connectés par quatre liaisons ; deux liaisons VSAT et deux liaisons VPN.

➔ Une interface va vers les agences. Elle se compose de 4 routeurs qui gèrent chacun les liaisons radios, les liaisons séries, la fibre optique et la liaison CXR filaire.

➔ Chaque agence est connectée au siège par deux liaisons de deux opérateurs différents selon les agences, l'une primaire et l'autre en backup.

➔ Les liaisons série et CXR sont fournies par Togocom et sont en cours de remplacement, soit par la fibre optique soit par la liaison radio.

2.2.2. Schéma de l'architecture du réseau de la BATG

Le réseau de la BATG se schématise comme dans la figure 5 :

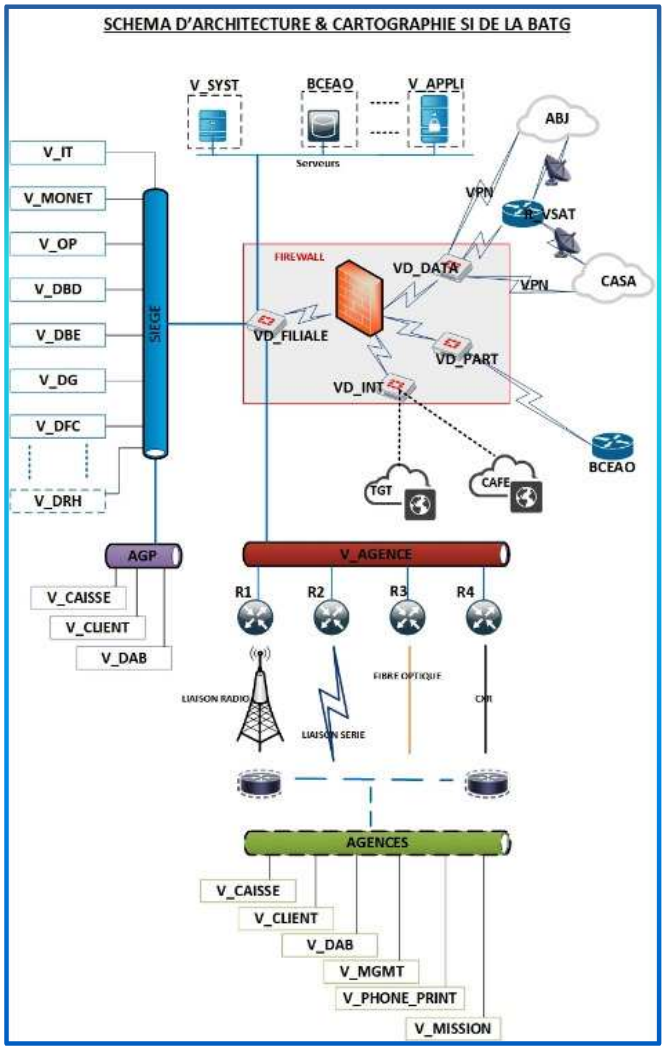


Figure 5: Schéma de l'architecture du réseau de la BATG.

Avec une infrastructure de cette envergure, la BATG en toute logique, a initié en 2016 le projet de l'installation d'un site de secours pour assurer la continuité de son activité.

2.2.3. Site de secours existant

Avant 2015, la majorité des serveurs nécessaires pour le métier étaient centralisés à Abidjan avec Cotonou comme site backup. En local, seul le serveur pour la « Compensation » était déployé. Mais au vu des besoins grandissant dans les filiales, les serveurs se sont localisés au fur et à mesure, et le besoin de continuité s'est également installé.

Ainsi, pour assurer la continuité de son activité, la BATG avait initié le projet de mise en place d'un site de repli en 2016.

La recommandation première d'ABI pour l'emplacement du site de secours est qu'il soit suffisamment distant de celui du site du siège (80 Km environ), et qu'il ne soit pas dans une zone de forte habitation. Mais compte tenu de la taille de la ville de Lomé qui est relativement petite, le choix de 80 Km n'est pas approprié. Du Nord au Sud, la ville s'étend sur 18 Km environ, et sur 33 Km d'Est en Ouest.

D'autre part, vu le réseau routier peu développé, il sera difficile d'installer un site backup trop loin de Lomé.

Ainsi, des propositions ont été faites pour des emplacements se trouvant dans la ville même de Lomé, car il fallait parer au plus pressé.

Ce site existe aujourd'hui et son aménagement est en cours et achevé à 84% environ. Le tableau 1, résume l'état d'avancement du projet d'aménagement de ce site :

Tableau 1 : Aménagement du site de repli existant.

Aménagement site repli et logistique	PRIORITE	REALISATION
Installation réseau électrique	1	OK
Installation de faux plancher surélevé	1	OK
Aménagement de la salle technique	1	OK
Acquisition de postes de travail	1	OK
Installation du système d'ondulation et de régulation électrique	1	OK
Présence agents de sécurité	1	OK
Installation du système de détection d'humidité et de déshumidification	2	Non prévu pour ce site provisoire
Installation de la climatisation	2	OK
Installation du système d'extinction d'incendie	2	OK
Installation de dispositifs de détection de chaleur	2	Non prévu pour ce site provisoire

Installation de dispositifs de détection de fumée et d'extinction automatique de feux	2	OK
Installation de groupe électrogène	3	OK
Installation des bureaux	3	OK
Mise en place de dispositifs de protection tels que des parafoudres ou des paratonnerres	3	OK
Acquisition de coffre ignifuge	3	OK
Certification du câblage électrique	3	OK
Installation de portes coupe-feux de la salle serveur	3	OK
Installation de détecteur d'inondation	3	Non prévu pour ce site provisoire
Installation de la vidéosurveillance	4	OK
Installation du contrôle d'accès	4	OK
Mise en place de dispositifs de réserve et de ravitaillement en carburant	5	OK
Validation de contrats de maintenance	5	NOK
Installations réseaux et télécom		
Acquisition de racks	1	OK
Réception des équipements VSAT	1	OK
Installation des équipements VSAT	1	La filiale est connectée pour l'instant par VPN
Installation du réseau informatique	1	OK
Test des installations VSAT	1	La filiale est connectée pour l'instant par VPN
Installation des équipements de sécurité	2	OK
Installation de liaisons internet redondées	2	OK
Installation téléphonie	3	NOK
Installation de la liaison backup avec le Datacenter ABI	3	OK
Switching des liaisons des agences vers le site de repli	3	NOK
Validation de contrats de maintenance	4	NOK
Installations des serveurs et applications		
Acquisition d'un serveur Active Directory	1	NOK

Installation du serveur Active Directory	1	NOK
Acquisition des serveurs infrastructures et métiers	3	OK
Installation des serveurs infrastructures et métiers	3	OK
Installation des applications métiers	4	OK

Cependant, ce site comporte un certain nombre d'inconvénients en plus de sa situation géographique non conforme :

- ➔ La colocation est un facteur limitant pour la maîtrise de l'environnement immédiat ; la cohabitation avec d'autres entreprises sont entre autres des raisons qui fragilisent la sécurité, les colocataires n'ayant pas nécessairement les mêmes exigences en matière de sécurité, une défaillance ou une négligence de leur part pourrait impacter le site de repli.
- ➔ La salle se situe au rez-de-chaussée.
- ➔ Le site est à proximité d'un grand marché de Lomé.
- ➔ Il est également situé en face d'une station d'essence.

En résumé, il s'agit d'un site de repli provisoire ou quelques services ont été dupliqués pour un certain nombre d'activités déterminées ainsi que des sauvegardes de serveurs.

Néanmoins, ceci ne s'inscrit pas dans le cadre de la mise en place d'une continuité globale de l'activité de la Banque. Dans les chapitres qui suivent, nous mettrons en place les procédures pour un plan de continuité d'activité globale de la banque Atlantique Togo, dans le cas où un sinistre surviendrait au siège de sa filiale.

CHAPITRE 3 : PCA POUR LA BATG

3.1. DÉFINITION DU PÉRIMÈTRE ET DES BESOINS EN CONTINUITÉ D'ACTIVITÉ

ABI a défini le périmètre comme regroupant toutes les fonctions de la filiale énumérées ci-dessous :

- ➔ Le métier (c'est à dire OPÉRATIONS, TRESORERIE, FINANCE et COMPTABILITE, BANQUE DE DETAIL, BANQUE DE L'ENTREPRISE).
- ➔ L'informatique et les télécoms.
- ➔ Les ressources humaines.
- ➔ La logistique.

3.1.1. Énumération des activités par service

Le point de départ d'un Plan de Continuité d'activité, est l'expression des besoins en continuité d'activités afin de pouvoir délimiter un périmètre. Il faut pour cela dans un premier temps, énumérer toutes les activités de tous les services de la banque afin d'identifier ceux qui sont essentiels pour la continuité en cas de sinistre.

La banque compte 11 directions et 4 services rattachés à la Direction Générale qui sont :

La Direction GENERALE,
La Direction des OPÉRATIONS (DO),
La Direction de la TRESORERIE,
La Direction de la FINANCE et COMPTABILITE (DFC),
La Direction de la BANQUE DE DETAIL (DBD),
La Direction de la BANQUE DE L'ENTREPRISE (DBE),
La Direction des ENGAGEMENTS (DE),
La Direction JURIDIQUE et GOUVERNANCE (DJG),
La Direction des RESSOURCES HUMAINES (DRH),
La Direction de l'AUDIT INTERNE (DAI),
La Direction des RISQUES et CONTRÔLE (DRC).

Les services rattachés à la Direction Générale :

Le Service INFORMATIQUE ET TECHNOLOGIE (IT),

Le Service ORGANISATION ET QUALITE (SOQ),
Le Service LOGISTIQUE et IMMOBILISATION,
Le Service COMMUNICATION ET MARKETING.

Après de nombreuses séances de travail avec chaque responsable de département/direction, les activités majeures de chaque service ont été recensées, classifiées et compilées dans le tableau 2 qui nous permettra par la suite de délimiter un périmètre pour les besoins en continuité d'activité :

Tableau 2 : Activités majeures par service.

DEPARTEMENT	LISTE DES SERVICES DANS LE DEPARTEMENT	ACTIVITES	LES PROCESSUS ASSOCIES
INFORMATION TECHNOLOGY	Support	• Support aux utilisateurs • Traitement de la compensation • Suivi du fonctionnement RTGS • Suivi de la gestion des applications digitales • Restauration des sauvegardes • Mise à jour des Bases de données • Traitement des applications de crédit (WORC) • Traitement des applications de dépassement/confirmation • Gestion du réseau de la banque • Tâches de basculement • Mise à jour des tables de routage • Mise à jour des règles	N/A
INFORMATION TECHNOLOGY	Exploitation Informatique		**Processus de la gestion de la compensation** : IT-Opérations-BCEAO-ABI **Processus de la gestion de RTGS :** Opérations -IT - ABI - BCEAO
INFORMATION TECHNOLOGY	Réseau Télécom et sécurité		**Processus Gestion de la disponibilité des Plateformes** : ABI – IT – Agences/Services - Utilisateur
TRESORERIE	Liquidité	•Transferts (Achat, vente de devises) •Emprunts •Placements (Titres, obligations)	**Processus de TRANSFERTS :** Client-Réception-Service étranger-gestionnaire-Trésorerie-Service étranger. **Processus d'Emprunts :** RTGS-SAGETIL-Dépôt manuel **Processus de Placements :** RTGS-SAGETIL
TRESORERIE	Sales		
DIRECTION JURIDIQUE ET GOUVERNANCE	Direction	•Conventions •Contrats •Garanties	N/A
DIRECTION JURIDIQUE ET GOUVERNANCE	Agents		N/A
DIRECTION FINANCIERE ET COMPTABLE	Service Comptabilité	•Ordonnancement des dépenses •Règlement des dépenses •Factures •Rapports •Rapports à la BCEAO	**Processus d'Ordonnancement des dépenses :** Moyens Généraux - Gestion financière - Direction Générale. **Processus de règlement des dépenses :** Moyens Généraux - DFC - DO - DG - DO
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle de Gestion		N/A

DIRECTION FINANCIERE ET COMPTABLE	Service Rapprochement		N/A
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle Comptable		
DIRECTION DES RESSOURCES HUMAINES	Service Gestion Prévisionnelle des Emplois	•Gestion prévisionnelle des emplois •Recrutements •Formations •Communication interne •Gestion des évaluations des performances du personnel •Élaboration des rapports RH (Bilan social, rapport d'activités)	N/A
DIRECTION DES RESSOURCES HUMAINES	Service Administration et paie	•Gestion administrative •Paiement des salaires •Paiement des taxes •Cotisations CNSS •Prise en charge Santé	N/A
ORGANISATION ET QUALITE	Service Organisation	•Gestion des projets SI •Mise en œuvre •Maintenance •Paramétrage des systèmes •Assistance aux utilisateurs •Gestion et suivi des réclamations	N/A
ORGANISATION ET QUALITE	Service Qualité		N/A
COMMUNICATIONS	Service Communications	•Gestion des communications de la Banque	N/A
DIRECTION DES OPERATIONS BANCAIRES	Service Étranger	•Transferts •CREDOC import-export •REMDOC import-export •Suivi règlementation (R08) •Back office TRESO •Rapports BCEAO, Ministère des finances	**PROCESSUS TRANSFERT :** Réception - DO - Chef service Étranger - Agent service Étranger - Chef service Étranger - DO (pour validation finale) **PROCESSUS CREDOC :** DBE - DE - CIC (ou CSC) - BCP **PROCESSUS REMDOC :** DBE - DBD - TRESO

DIRECTION DES OPERATIONS BANCAIRES	Service Back Office Monétique	•Gestion des transferts d'argent •Gestion des guichets automatiques et des cartes •Gestion des réclamations •Réconciliation des comptes monétiques •M-Banking •Réconciliation des comptes des cartes internationales	**PROCESSUS RECLAMATIONS** : Agence - réception/courrier - DG - DO - Monétique - agence (par courrier) **PROCESSUS TRANSFERTS :** Agents commerciaux - Front office - Gestionnaire de transfert rapide **Gestion des guichets automatiques :** Charges de clientèle - Service BO Monétique **PROCESSUS M-BANQUING :** MOOV - R.O. Qualité - Gestionnaire de transfert rapide
DIRECTION DES OPERATIONS BANCAIRES	Service Portefeuille	•Réception et dispatching de tous les ordres (Virements, chèques, etc..) •Gestion des virements •Gestion des chèques •Génération des fichiers salaires •1ere et 2eme Validation portefeuille local •Dépouillement et dispatching des messages RTGS et SWIFT	**PROCESSUS VIREMENTS :** Réception - DO - Chef Service Portefeuille ou DO (selon le montant pour validation) **PROCESSUS CHEQUES** : Réception par l'agent clientèle/mail/agence/poste/bornes - agent Service Portefeuille (pour traitement) **Validation portefeuille local :** Monétique - Service Étranger - CAD - Caisse
DIRECTION DES OPERATIONS BANCAIRES	Service Contrôle des Opérations	•Vérification des Operations comptables	N/A
DIRECTION DES OPERATIONS BANCAIRES	Caisse	•Opérations de dépôts •Opérations de retraits •Opérations de Transfert d'argent •Achat et vente de devises	N/A
DIRECTION RISQUE ET CONTRÔLE	Service Contrôle Permanent	•Contrôle •Détection et enregistrement des incidents	N/A
DIRECTION RISQUE ET CONTRÔLE	Service Conformité	•Gestion de la conformité •Réquisitions •Profilage et filtrage de la clientèle •Filtrage des transactions	**PROCESSUS Courrier de réponse ou réquisition venant de CENTIF :** Réception courrier - DG - DRC - Service conformité - DRC - Transmission à la CENTIF **PROCESSUS REQUETE Correspondant bancaire :** DO (pour réception) - Charge de clientèle (pour traitement) - DO - Service Conformité (pour vérification physique des informations données) - DRC (pour validation) - Service Conformité - DO (pour transmission)

DIRECTION RISQUE ET CONTRÔLE	Risque Management	•Déclaration et collecte des incidents •Validation de la cartographie des risques •Gestion des risques	**PROCESSUS Déclaration et collecte des incidents** : Contrôle Permanent (Pour détection et enregistrement) - Risques (Pour validation et mise à jour de la cartographie des risques)
DIRECTION BANQUE DE L'ENTREPRISE	Service Grandes Entreprises	•Gestion des dépassements •Confirmation •Crédit aux entreprises •Prospection des clients •Développement de la relation client •Montage de dossier de crédit aux entreprises •CREDOC/REMDOC aux entreprises	**PROCESSUS DE DEPASSEMENT** : Caisse ou agent des Opérations = initiateur - Gestionnaire - DBE/DBD - DE (Risques) - CAD (Contrôle admin du crédit - caisse ou agent des Opérations = initiateur) **PROCESSUS DE CONFIRMATION** : Caisse ou agent des Opérations = initiateur - Gestionnaire - initiateur
DIRECTION BANQUE DE L'ENTREPRISE	Service Institutionnels États et démembrements		
DIRECTION BANQUE DE L'ENTREPRISE	Service Local Corporate PME - PMI		
DIRECTION BANQUE DE L'ENTREPRISE	Service Cash Management & Trade		
SERVICE LOGISTIQUES ET IMMOBILISATION	Chef Service		**PROCESSUS ACHATS:** Service demandeur (expression du besoin) - SLI (pour initier l'achat) - Fournisseur (pour les factures pro-forma) - Contrôleur de gestion (pour l'imputation dans l'application budgétaire) - Impression - Chargé des achats - Chef SLI - Contrôleur de gestion - DFC- DO - DG - SLI (pour le bon de commande) - Chargé des achats - Chef SLI - DO - DFC - DG - fournisseur (pour la livraison) - SLI - fournisseur (pour dépôt de facture) - SLI (pour paiement) - Comptabilité - DFC - DO - DG - Comptabilité - DO (pour saisie dans Orion) **PROCESSUS GESTION DES ACCES :** Départements - SLI
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Logistique	•Gestion de la logistique •Achats •Bons de commande •Gestion des fournisseurs	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Immobilisation		
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Sécurité	•Gestion de la Sécurité physique	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Archives	•Archivage des documents de la Banque	N/A
DIRECTION AUDIT INTERNE		•Audits interne	N/A
DIRECTION ENGAGEMENTS	Service Administration des engagements	•Gestion administrative des engagements •Suivi des créances en souffrance non	**PROCESSUS OCTROI DE CREDIT** : Commercial - DE (pour la contre étude) - Comité de Crédit (DG, DBE,

DIRECTION ENGAGEMENTS	Service Contre-étude ou Analyse de Crédit	contentieuses •Analyse des crédits •Gestion de l'état des engagements conformément aux contrats •Rapports aux autorités monétaires •Rapports statistiques périodiques d'engagement de crédit •Recouvrements	DBD, DE) - Gestionnaire - Client - DJG - Administration des engagements (pour introduction dans le système et mise en place) - DO (pour validation)
DIRECTION ENGAGEMENTS	Service Surveillance des engagements		
DIRECTION ENGAGEMENTS	Service Recouvrement		
DIRECTION BANQUE DE DETAIL	Service Produits	•Vente des produits de la banque : Offres packagées, Cartes, Épargnes et classement, Bancassurance, transfert d'argent •Assistance clientèle	N/A
DIRECTION BANQUE DE DETAIL	Agences		
DIRECTION BANQUE DE DETAIL	Gestionnaires de comptes		

Ainsi, nous avons établi une liste exhaustive de toutes les activités des départements et directions de la Banque. Afin de déterminer celles qui sont essentielles à la continuité d'activités, nous allons à présent étudier l'impact de leur arrêt et les classifier en leur attribuant à chacun un poids.

3.1.2. Identification et management des processus métiers et impacts financiers de leur arrêt

L'impact de l'arrêt des activités essentielles et de leurs processus associés sur certains départements est qualitatif et ne peut pas réellement être chiffré. En prenant l'exemple du département IT (l'exploitation précisément), l'indisponibilité de ce département entrainera l'arrêt de presque toutes les activités de la Banque y compris les mails, les applications métiers, les sites de production distants, le lien avec les agences, les transmissions de certaines opérations, etc. Pour chiffrer son impact, il faudrait additionner les pertes de la majorité des départements de la Banque. Il en est de même pour la plupart des départements qui servent de support, tels que la Direction des Opérations, la Direction Financière et comptable, la Direction Juridique et Gouvernance, pour ne citer que celles-là.

La classification que nous avions voulu faire se base sur le poids financier de chaque département de la banque, c'est-à-dire la contribution de chaque service au chiffre d'affaires global de la banque, et ce, journalièrement. Ceci nous permettrait de spécifier clairement à la Direction Générale, le manque à gagner de la banque en cas d'arrêt complet de l'activité de chacun des départements pendant quelques heures. [6]

Malheureusement, ces statistiques n'étaient pas disponibles. Il ne nous a donc pas été possible de déterminer sur une chaine de processus, quelle quote-part financière attribuer à chaque département impliqué.

La méthodologie que nous avons donc choisi de suivre pour estimer le poids des départements se base sur l'évaluation des processus, et est la suivante :

- ➔ 31 processus critiques ont été recensés lors de la collecte d'informations dans chaque département. Nous avons analysé chaque processus et dénombré chaque fois qu'un département intervenait.

- ➔ Dans le tableau 3, nous avons fait la liste des processus essentiels dans lesquels interviennent les départements :

Tableau 3 : Processus essentiels par département.

INDEX	DEPARTEMENT	PROCESSUS	DEPARTEMENT INTERVENANT DANS LES PROCESSUS
1	INFORMATION TECHNOLOGY	**Processus de la gestion de la compensation**	IT-Opérations-BCEAO (par la plateforme IT) -ABI (par la plateforme IT)
2	INFORMATION TECHNOLOGY	**Processus de la gestion de RTGS**	Opérations -IT – ABI (par la plateforme IT) – BCEAO (par la plateforme IT)
3	INFORMATION TECHNOLOGY	**Processus de Gestion de la disponibilité des Plateformes**	ABI – IT – Agences/Services - Utilisateur
4	TRESORERIE	**Processus de TRANSFERTS**	Client-Réception-Service étranger-gestionnaire-Trésorerie-Service étranger
5	TRESORERIE	**Processus d'Emprunts**	RTGS-SAGETIL-Dépôt manuel-Intervention IT
6	TRESORERIE	**Processus de Placements**	RTGS-SAGETIL- Intervention IT
7	DIRECTION FINANCIERE ET COMPTABLE	**Processus d'Ordonnancement des dépenses**	Moyens Généraux - Gestion financière - Direction Générale
8	DIRECTION FINANCIERE ET COMPTABLE	**Processus de règlement des dépenses**	Moyens Généraux - DFC - DO - DG - DO
9	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS REMDOC**	DBE - DBD - TRESO
10	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS TRANSFERT**	Réception - DO - Chef service Étranger - Agent service Étranger - Chef service Étranger - DO (pour validation finale)
11	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS CREDOC**	DBE - DE - CIC (ou CSC) - BCP
12	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS RECLAMATIONS**	Agence - réception/courrier - DG - DO - Monétique - agence (par courrier)
13	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS CHEQUES**	Réception par l'agent clientèle/mail/agence/poste/bornes - agent Service Portefeuille (pour traitement) - Intervention IT pour serveur ACS corporate
14	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS TRANSFERTS**	Agents commerciaux - Front office - Gestionnaire de transfert rapide
15	DIRECTION DES OPERATIONS BANCAIRES	**Gestion des guichets automatiques**	Charges de clientèle - Service BO Monétique- IT (pour gestion des GAB)

16	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS M-BANQUING**	MOOV - R.O. Qualité - Gestionnaire de transfert rapide-IT (pour réconciliation)
17	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS VIREMENTS**	Réception - DO - Chef Service Portefeuille ou DO (selon le montant pour validation) -IT (pour intégration de fichier)
18	DIRECTION DES OPERATIONS BANCAIRES	**Validation portefeuille local**	Monétique - Service Étranger - CAD - Caisse
19	DIRECTION RISQUE ET CONTRÔLE	**PROCESSUS Courrier de réponse ou réquisition venant de CENTIF**	Réception courrier - DG - DRC - Service conformité - DRC - Transmission à la CENTIF
20	DIRECTION RISQUE ET CONTRÔLE	**PROCESSUS REQUETE Correspondant bancaire**	DO (pour réception) - Charge de clientèle (pour traitement) - DO - Service Conformité (pour vérification physique des informations données) - DRC (pour validation) - Service Conformité - DO (pour transmission)
21	DIRECTION RISQUE ET CONTRÔLE	**PROCESSUS Déclaration et collecte des incidents**	Contrôle Permanent (Pour détection et enregistrement) - Risques (Pour validation et mise à jour de la cartographie des risques)
22	DIRECTION BANQUE DE L'ENTREPRISE	**PROCESSUS DE CONFIRMATION**	Caisse ou agent des Opérations = initiateur - Gestionnaire – initiateur- IT (pour gestion des habilitations) - IT pour serveur dépassement / confirmation
23	DIRECTION BANQUE DE L'ENTREPRISE	**PROCESSUS DE DEPASSEMENT**	Caisse ou agent des Opérations = initiateur - Gestionnaire - DBE/DBD - DE (Risques) - CAD (Contrôle admin du crédit - caisse ou agent des Opérations = initiateur) - IT (pour gestion des habilitations) - IT pour serveur dépassement / confirmation
24	SERVICE LOGISTIQUES ET IMMOBILISATION	**PROCESSUS ACHATS**	Service demandeur (expression du besoin) - SLI (pour initier l'achat) - Fournisseur (pour les factures pro-forma) - Contrôleur de gestion (pour l'imputation dans l'application budgétaire) - Impression - Chargé des achats - Chef SLI - Contrôleur de gestion - DFC- DO - DG - SLI (pour le bon de commande) - Chargé des achats - Chef SLI - DO - DFC - DG - fournisseur (pour la livraison) - SLI - fournisseur (pour dépôt de facture) - SLI (pour paiement) - Comptabilité - DFC - DO - DG - Comptabilité - DO (pour saisie dans Orion)

25	SERVICE LOGISTIQUES ET IMMOBILISATION	**PROCESSUS GESTION DES ACCES**	Départements - SLI
26	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS RETRAIT DE FONDS A LA BCEAO**	Caissier (initiateur)-DO- TRESO pour approbation
27	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS DEPOT DE FONDS A LA BCEAO**	Caissier – DO- TRESO
28	DIRECTION DES OPERATIONS BANCAIRES	**PROCESSUS ACHAT ET VENTE DE DEVISES**	Client-Caissier (initiateur)- TRESO (pour le taux de change) - caissier-client
29	DIRECTION BANQUE DE DETAIL	**PROCESSUS DE CONFIRMATION**	Caisse ou agent des Opérations = initiateur - Gestionnaire – initiateur- IT (pour gestion des habilitations) - IT pour serveur dépassement / confirmation
30	DIRECTION BANQUE DE DETAIL	**PROCESSUS DE DEPASSEMENT**	Caisse ou agent des Opérations = initiateur - Gestionnaire - DBE/DBD - DE (Risques) - CAD (Contrôle admin du crédit - caisse ou agent des Opérations = initiateur) - IT (pour gestion des habilitations) - IT pour serveur dépassement / confirmation
31	DIRECTION ENGAGEMENTS	**PROCESSUS OCTROI DE CREDIT**	Commercial - DE (pour la contre étude) - Comité de Crédit (DG, DBE, DBD, DE) - Gestionnaire - Client - DJG - Administration des engagements (pour introduction dans le système et mise en place) - DO (pour validation) - Intervention IT

Les ajouts en couleur bleue sont les interventions d'IT dans les différents processus remontés par les départements.

La figure 6 nous décrit un exemple d'étapes d'un processus métier.

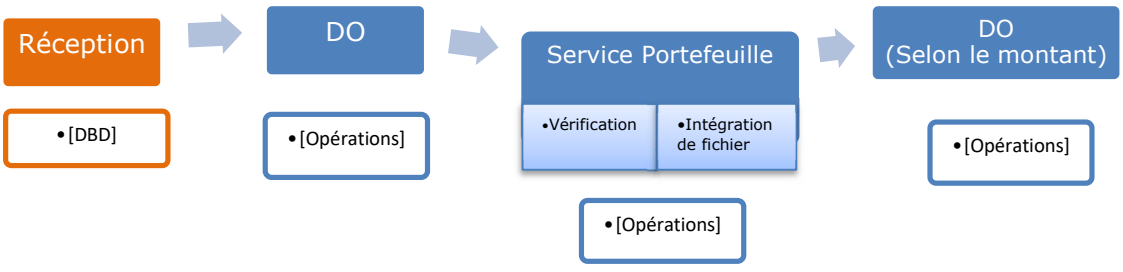


Figure 6 : Exemple d'un processus métier : PROCESSUS VIREMENT.

➔ Le processus est un ensemble d'activités corrélées et en interactions conçu pour arriver à un résultat donné. L'une doit se faire avant que l'autre ne puisse s'exécuter.

➔ Nous faisons ensuite le pourcentage d'interventions par rapport au nombre global d'entrées pour chaque département.

➔ Le tableau 4 résume les interventions de chaque département dans l'exécution des processus métiers :

Tableau 4: Interventions par département dans les processus critiques de la banque.

DEPARTEMENT	NOMBRE D'INTERVENTIONS DANS LES PROCESSUS	POURCENTAGES
INFORMATION TECHNOLOGY	24	17%
TRESORERIE	7	5%
DIRECTION JURIDIQUE ET GOUVERNANCE	1	1%
DIRECTION FINANCIERE ET COMPTABLE	9	6%
DIRECTION DES RESSOURCES HUMAINES	0	0%
ORGANISATION ET QUALITE	0	0%
COMMUNICATIONS	0	0%
DIRECTION DES OPERATIONS BANCAIRES	41	29%
DIRECTION RISQUE ET CONTRÔLE	7	5%
DIRECTION BANQUE DE L'ENTREPRISE	4	3%
SERVICE LOGISTIQUES ET IMMOBILISATION	11	8%
DIRECTION AUDIT INTERNE	0	0%
DIRECTION ENGAGEMENTS	9	6%
DIRECTION BANQUE DE DETAIL	21	15%
DIRECTION GENERALE	8	6%
	142	100%

➔ Nous introduisons ensuite ces chiffres dans le tableau des contributions de chaque département au chiffre d'affaires global de la banque. Cela constitue les poids de chaque département.

➔ Nous obtenons le tableau de pondération (Tableau 5) :

Tableau 5: Pondération par service.

DEPARTEMENT	TYPE D'IMPACT	PRODUIT NET BANCAIRE 2019	PONDERATION (en fonction des Processus critiques) P	Formule proposée de l'évaluation du cout théorique d'un incident sur un département spécifique : (C X P) /240 jours ouvrés (pour 24h)
INFORMATION TECHNOLOGY	Qualitatif	10,346,000,000,000	16.90%	7,285,915,493
TRESORERIE	Quantitatif	10,346,000,000,000	4.93%	2,125,058,685
DIRECTION JURIDIQUE ET GOUVERNANCE	Qualitatif	10,346,000,000,000	0.70%	303,579,812
DIRECTION FINANCIERE ET COMPTABLE	Qualitatif	10,346,000,000,000	6.34%	2,732,218,310
DIRECTION DES OPERATIONS BANCAIRES	Qualitatif	10,346,000,000,000	28.87%	12,446,772,300
DIRECTION RISQUE ET CONTRÔLE	Qualitatif	10,346,000,000,000	4.93%	2,125,058,685
DIRECTION BANQUE DE L'ENTREPRISE	Quantitatif	10,346,000,000,000	2.82%	1,214,319,249
SERVICE LOGISTIQUES ET IMMOBILISATION	Qualitatif	10,346,000,000,000	7.75%	3,339,377,934
DIRECTION ENGAGEMENTS	Qualitatif	10,346,000,000,000	6.34%	2,732,218,310
DIRECTION BANQUE DE DETAIL	Quantitatif	10,346,000,000,000	14.79%	6,375,176,056
DIRECTION GENERALE	Qualitatif	10,346,000,000,000	5.63%	2,428,638,498
			100%	**43,108,333,333**

DEPARTEMENT	TYPE D'IMPACT	PONDERATION (en fonction des Processus critiques) P
DIRECTION DES RESSOURCES HUMAINES	Qualitatif	Pas de processus critiques remontés
ORGANISATION ET QUALITE	Qualitatif	Pas de processus critiques remontés
COMMUNICATIONS	Qualitatif	Pas de processus critiques remontés
DIRECTION AUDIT INTERNE	Qualitatif	Pas de processus critiques remontés

Chaque département y est représenté avec un pourcentage qui est fonction du nombre de ses interventions dans les processus critiques de la banque.

Les 4 Directions et départements ci-dessus n'ont pas de pondération car ils n'ont pas remonté de processus. Cela ne signifie pas qu'ils ne sont pas critiques à la banque,

mais, étant donné qu'ils n'interviennent que très peu ou pas dans les processus critiques, ils ne sont pas obligatoirement à maintenir immédiatement dans le cadre d'une continuité d'activité de la banque après un sinistre grave. Les membres de ces Directions et départements peuvent continuer à assurer leurs tâches en télétravail à partir de leurs domiciles respectifs.

La figure 7 nous donne une représentation graphique des pourcentages sus- cités.

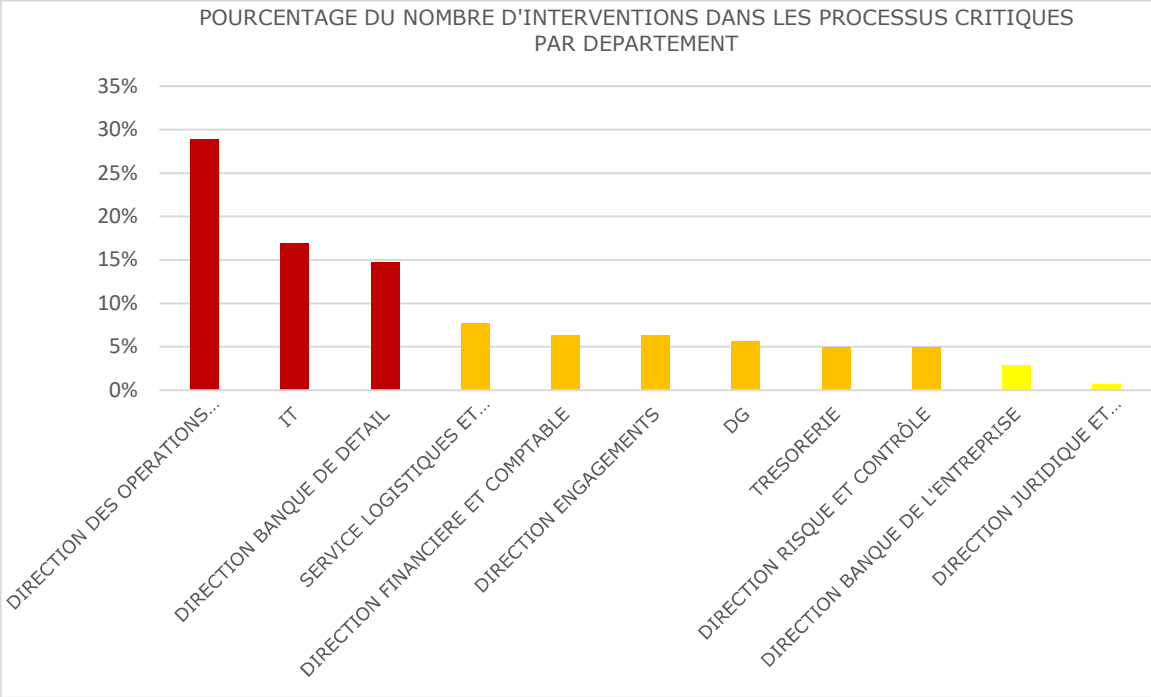


Figure 7 : Pourcentage par département dans les processus critiques.

Ainsi, certaines activités des départements et directions OPÉRATIONS, IT, BANQUE DE DETAIL ont été jugées les plus critiques et essentielles à l'accomplissement des objectifs de la banque dans le cadre d'un PCA suite à un sinistre important.

Les activités des départements et directions LOGISTIQUE et IMMOBILISATION, FINANCIERE et COMPTABLE, ENGAGEMENTS, GENERALE, TRESORERIE, RISQUES et CONTROLE, ont été jugées moyennement critiques.

Les activités des départements et directions, BANQUE DE L'ENTREPRISE, JURIDIQUE et GOUVERNANCE, RESSOURCES HUMAINES, ORGANISATION et QUALITE, COMMUNICATIONS, AUDIT INTERNE ont été jugées moins critiques.

Les impacts principaux de l'arrêt des activités essentielles sont résumés dans le tableau 6 :

Tableau 6: Impacts de l'arrêt des activités essentielles.

DEPARTEMENT	LISTE DES SERVICES DANS LE DEPARTEMENT	ACTIVITES	IMPACT FINANCIER	IMPACT (Commentaires recueillis)
INFORMATION TECHNOLOGY	Support	• Support aux utilisateurs • Traitement de la compensation • Suivi du fonctionnement RTGS • Suivi de la gestion des applications digitales • Restauration des sauvegardes • Mise à jour des Bases de données • Traitement des applications de crédit (WORC) • Traitement des applications de dépassement / confirmation • Gestion du réseau de la banque • Tâches de basculement • Mise à jour des tables de routage • Mise à jour des règles	7,285,915,493	Arrêt de l'assistance aux utilisateurs
INFORMATION TECHNOLOGY	Exploitation Informatique			Arrêt de toutes les applications et des serveurs
INFORMATION TECHNOLOGY	Réseau Télécom et sécurité			Arrêt de la connexion réseau et Internet
TRESORERIE	Liquidité	•Transferts (Achat, vente de devises) •Emprunts •Placements (Titres, obligations)	2,125,058,685	Arrêt des emprunts interbancaires, perte des revenus net de change, perte des gains sur les portefeuilles
TRESORERIE	Sales			
DIRECTION JURIDIQUE ET GOUVERNANCE	Direction	•Conventions •Contrats •Garanties	303,579,812	
DIRECTION JURIDIQUE ET GOUVERNANCE	Agents			
DIRECTION FINANCIERE ET COMPTABLE	Service Comptabilité	•Ordonnancement des dépenses •Règlement des dépenses •Factures •Rapports •Rapports à la BCEAO	2,732,218,310	Arrêt du reporting a la BCEAO Pénalités Arrêt de paiement des factures Image de la banque
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle de Gestion			
DIRECTION FINANCIERE ET COMPTABLE	Service Rapprochement			
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle Comptable			
DIRECTION DES RESSOURCES HUMAINES	Service Gestion Prévisionnelle des Emplois	•Gestion prévisionnelle des emplois •Recrutements •Formations •Communication interne •Gestion des évaluations des performances du personnel •Élaboration des rapports RH (Bilan social, rapport d'activités)	-	Image de la Banque

DIRECTION DES RESSOURCES HUMAINES	Service Administration et paie	•Gestion administrative •Paiement des salaires •Paiement des taxes •Cotisations CNSS •Prise en charge Santé		Salaires affectés
ORGANISATION ET QUALITE	Service Organisation	•Gestion des projets SI •Mise en œuvre •Maintenance •Paramétrage des systèmes •Assistance aux utilisateurs •Gestion et suivi des réclamations	-	
ORGANISATION ET QUALITE	Service Qualité			
COMMUNICATIONS	Service Communications	•Gestion des communications de la Banque	-	Image de la Banque Clients mécontents
DIRECTION DES OPERATIONS BANCAIRES	Service Étranger	•Transferts •CREDOC import-export •REMDOC import-export •Suivi règlementation (R08) •Back office TRESO •Rapports BCEAO, Ministère des finances	12,446,772,300	
DIRECTION DES OPERATIONS BANCAIRES	Service Back Office Monétique	•Gestion des transferts d'argent •Gestion des guichets automatiques et des cartes •Gestion des réclamations •Réconciliation des comptes monétiques •M-Banking •Réconciliation des comptes des cartes internationales		
DIRECTION DES OPERATIONS BANCAIRES	Service Portefeuille	•Réception et dispatching de tous les ordres (Virements, chèques, etc..) •Gestion des virements •Gestion des chèques •Génération des fichiers salaires •1ere et 2eme Validation portefeuille local •Dépouillement et dispatching des messages RTGS et SWIFT		
DIRECTION DES OPERATIONS BANCAIRES	Service Contrôle des Opérations	•Vérification des Operations comptables		Non secouru
DIRECTION DES OPERATIONS BANCAIRES	Caisse	•Opérations de dépôts •Opérations de retraits •Opérations de Transfert d'argent •Achat et vente de devises		Arrêt des opérations de dépôts, retraits uniquement par carte et plus pour les particuliers ; Problème de retrait pour les entreprises Perte des commissions de Transfer d'argent
DIRECTION RISQUE ET CONTRÔLE	Service Contrôle Permanent	•Contrôle •Détection et enregistrement des incidents	2,125,058,685	
DIRECTION RISQUE ET CONTRÔLE	Service Conformité	•Gestion de la conformité •Réquisitions •Profilage et filtrage de la clientèle •Filtrage des transactions		

DIRECTION RISQUE ET CONTRÔLE	Risque Management	•Déclaration et collecte des incidents •Validation de la cartographie des risques •Gestion des risques		
DIRECTION BANQUE DE L'ENTREPRISE	Service Grandes Entreprises	•Gestion des dépassements •Confirmation •Crédit aux entreprises •Prospection des clients •Développement de la relation client •Montage de dossier de crédit aux entreprises •CREDOC/REMDOC aux entreprises	1,214,319,249	Arrêt des Pipeline deals. Plus de crédits aux entreprises, donc perte des intérêts
DIRECTION BANQUE DE L'ENTREPRISE	Service Institutionnels Etats et démembrements			
DIRECTION BANQUE DE L'ENTREPRISE	Service Local Corporate PME - PMI			
DIRECTION BANQUE DE L'ENTREPRISE	Service Cash Management & Trade			
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Logistique	•Gestion de la logistique •Achats •Bons de commande •Gestion des fournisseurs	3,339,377,934	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Immobilisation			
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Sécurité	•Gestion de la Sécurité physique		
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Archives	•Archivage des documents de la Banque		Non secouru
DIRECTION AUDIT INTERNE	Direction Audit Interne	•Audits interne	-	
DIRECTION ENGAGEMENTS	Service Administration des engagements	•Gestion administrative des engagements •Suivi des créances en souffrance non contentieuses •Analyse des crédits •Gestion de l'état des engagements conformément aux contrats •Rapports aux autorités monétaires •Rapports statistiques périodiques d'engagement de crédit •Recouvrements	2,732,218,310	
DIRECTION ENGAGEMENTS	Service Contre-étude ou Analyse de Crédit			
DIRECTION ENGAGEMENTS	Service Surveillance des engagements			
DIRECTION ENGAGEMENTS	Service Recouvrement			Non secouru
DIRECTION BANQUE DE DETAIL	Service Produits	•Vente des produits de la banque : Offres packagées, Cartes, Épargnes et classement, Bancassurance, transfert d'argent •Assistance clientèle	6,375,176,056	Les agences n'ont pas de sinistre, et les gestionnaires sont la
DIRECTION BANQUE DE DETAIL	Agences			
DIRECTION BANQUE DE DETAIL	Gestionnaires de comptes			

Interprétation : On estime ainsi que :

La banque perd 7 285 915 493 de FCFA de chiffre d'affaires par jour si la plateforme IT n'est pas disponible.

Elle perd 6 375 176 056 de FCFA par jour si les agences et leurs gestionnaires ne peuvent pas accéder au siège.

Elle perd 12 446 772 300 de FCFA par jour si les Opérations ne fonctionnent pas.

Pour limiter ces pertes, il faut que l'activité de la banque ne soit pas interrompue. Les risques qu'encourt la banque doivent donc être analysés et cartographiés afin de trouver des moyens de limiter leur occurrence et de définir une stratégie de continuité de ses activités. C'est l'objectif du paragraphe suivant.

3.1.3. Analyse des Risques et Cartographie pour les activités et les processus critiques

Dans le domaine de la gestion des risques, l'évaluation des risques est l'ensemble des méthodes consistant à chiffrer la criticité des dangers. Elle vise à les qualifier et à les quantifier. Ils doivent donc préalablement avoir été identifiés. On se restreint ici à l'étude en ne considérant que les événements à conséquences négatives. On s'attache à obtenir des indices de risque (ou quotient de risque) traduits en valeurs chiffrées, pour classer les risques en les hiérarchisant afin de pouvoir prioriser les mesures à prendre pour les réduire et/ou atténuer leurs conséquences ou rendre le risque acceptable. [7]

La gestion des risques a ainsi pour objectif général de diminuer les effets de l'incertitude pour atteindre les objectifs. Elle permet en outre de mieux connaître les conséquences possibles ainsi que leur probabilité d'occurrence et donc de définir raisonnablement la stratégie de continuité d'activité. [8]

On identifie ainsi les scénarios de crise qui justifient une démarche de continuité.

3.1.3.1. Procédure d'analyse de risques

Nous procèderons ici, à une analyse qualitative des risques en nous inspirant de la méthode EBIOS [9] (Expression des Besoins et Identification des Objectifs de Sécurité). La procédure de notre analyse de risques comporte 4 étapes :

- ➔ Identifier les risques de toute nature.
- ➔ Analyser ces risques selon les critères de gravité et de probabilité d'occurrence (Le terme anglais « likelihood » (vraisemblance) n'a pas d'équivalent direct en français et c'est souvent l'équivalent du terme « probability » (probabilité) qui est utilisé à la place. C'est pourquoi, le terme « probabilité » représente plutôt ici un indice de vraisemblance qu'un évènement se produise, et des chiffres entiers de 1 à 5 sont ainsi utilisés). [9]
- ➔ Évaluer en fonction du contexte et des enjeux de la banque.
- ➔ Les traiter pour limiter leur impact et leur probabilité.

3.1.3.2. Cartographie des risques

Dans le cadre de notre cartographie de risques pour la BATG, nous sélectionnons différents scénarios. Pour chaque scénario finalement retenu dans le PCA, nous indiquons les mesures particulières de prévention ou de protection, les impacts principaux, les probabilités et le niveau de risque ainsi que l'ordre de priorité de traitement.

Par définition, le risque se détermine comme suit :

RISQUE= PROBABILITE X IMPACT

Le tableau 10 présente la cartographie des risques retenus pour la BATG ; le tableau 7 représente les échelles de valeurs de probabilité et d'impact ; le tableau 8 est la synthèse Probabilité X Impact et le tableau 9 est le niveau de risque.

Tableau 7 : Probabilité et Impact.

PROBABILITE		
1	Improbable	Ne se produit jamais ou très rarement dans la zone
2	Rare	Moins d'une fois/an
3	Occasionnel	2 à 3 fois/an
4	Fort	3 à 4 fois/an
5	Très fort	5 fois et plus /an

IMPACT		
1	Négligeable	Non important
2	Bas	Pas une priorité
3	Modéré	Risque gérable, doit être atténué
4	Critique	Mesures à évaluer et solutions à mettre en place. Revue 1/an
5	Catastrophique	Mesures à évaluer et solutions rapides à mettre en place. Revue 2/an

Tableau 8 : Synthèse = Probabilité X Impact.

IMPACT	**PROBABILITE**				
		Improbable (1)	Rare (2)	Occasionnel (3)	Fort (4)	Très fort (5)
	Catastrophique (5)	5	10	15	20	25
	Critique (4)	4	8	12	16	20
	Modéré (3)	3	6	9	12	15
	Bas (2)	2	4	6	8	10
	Négligeable (1)	1	2	3	4	5

Tableau 9: Niveau de risque.

Niveau de risque	
1-6	Bas
7-9	Moyen
10-14	Élevé
15-25	Très élevé

Tableau 10: Cartographie des risques pour la BATG.

SCENARIO DE RISQUES	ACRONYME	DESCRIPTION	CONSEQUENCES	PROBABILITE	IMPACT	Niveau de Risque	Ordre de priorité de traitement	Mesure préventives et curatives
Accident industriel	AI	Problème dans une usine ou une station d'essence environnante (Explosions, gaz, feu…etc.)	Inaccessibilité du siège	1	4	4	3	•Activation du télétravail
Mouvements sociaux	MS	•Inaccessibilité de l'infrastructure par suite de conflit social •Coupure/indisponibilité de voies de communication rendant l'accès impossible •Suspension d'Internet par les autorités	Inaccessibilité du siège	3	2	6	3	•Activation du déplacement vers le site de repli
Défaillance prestataire essentiel	DP	•Indisponibilité des fournisseurs d'accès Internet •Indisponibilité des fournisseurs de fibre optique •Indisponibilité des fournisseurs de réseau filaire •Indisponibilité des fournisseurs de Boucle Locale Radio	•Impossibilité d'accomplir les activités essentielles •Pertes financières	3	5	15	1	•Basculement vers les Fournisseurs de secours sur la liaison redondante •Activation du déplacement vers le site de repli
Panne électrique prolongée	PE	•Indisponibilité VSAT •Panne de secteur prolongée •Panne du système de climatisation dans la salle serveur •Panne électrique dans la salle serveur •Réseau électrique instable	•Dysfonctionnement des serveurs •Arrêt des serveurs •Impossibilité d'accomplir les activités essentielles •Pertes financières	2	3	6	3	•Deux circuits ondulés alimentent la salle •Activation du générateur de secours ou de son backup
Inondation	IN	•Risques d'inondation dans l'immeuble •Risque du a la proximité de la mer •Dégâts d'eau sur le matériel	•Indisponibilité du siège	2	3	6	3	•Activation du déplacement vers le site de repli

Cyber-attaque	CA	•Indisponibilité du système d'information par suite d'intrusion à travers les réseaux à des fins malveillantes (Blocage du réseau télécom, rançongiciel, Virus, Intrusion logicielle…etc.)	•Interruption de service IT •Impossibilité temporaire d'accomplir les activités essentielles •Pertes financières •Vol de données stratégiques	2	4	8	2	•Séparation claire des domaines •Isolation de la zone d'attaque •Mise en service des serveurs backup •Procédure à suivre en cas de rançongiciel
Catastrophes naturelles	CN	Inaccessibilité de l'infrastructure par suite de catastrophe naturelle : •Perturbations météorologiques graves (tempêtes, cyclones, tornades, orages violents) •Températures extrêmes •Changement climatique •Raz-de-marée •Rayonnements électromagnétiques ou thermiques	•Indisponibilité du siège	2	5	10	2	•Activation du déplacement vers le site de repli
Panne Telecom prolongée	PT	•Panne des VSAT •Panne matérielle télécom (radios, antennes…) •Panne des Fournisseurs essentiels	•Interruption de service IT •Impossibilité d'accomplir les activités essentielles •Pertes financières	2	4	8	2	•Basculement sur les liaisons de secours •Convention avec un autre fournisseur en backup •Activation du déplacement vers le site de repli
Attentat explosif	AE	Inaccessibilité de l'infrastructure par suite d'acte de terrorisme	•Indisponibilité du siège	1	3	3	3	•Activation du déplacement vers le site de repli
Absence de contrat de maintenance sur l'infrastructure	ACM	•Absence de contrats d'entretien des infrastructures électriques •Absence de contrats de maintenance du parc Informatique	•Arrêt de service •Défaillance des équipements •Dégradation du service •Risque d'incendie du a la vétusté de certaines installations	3	4	12	1	•Signer des contrats avec un cabinet ou des prestataires dans le domaine de l'Ingénierie Électrique et Informatique •Activation et basculement sur le site de repli
Pandémie/Épidémie/ Problème sanitaire majeur	P	Indisponibilité du personnel consécutive à une pandémie	•Indisponibilité des employés du siège •Impossibilité d'accomplir les activités essentielles •Pertes financières •Image de la Banque	3	4	12	1	•Activation du télétravail

Défaillance technique	DT	•Panne de matériel critique (Routeurs, serveurs, onduleurs, générateur de secours) •Dysfonctionnement d'un logiciel critique	•Interruption de service IT •Impossibilité d'accomplir les activités essentielles •Pertes financières	2	3	6	3	•Parafoudre •Paratonnerre •Onduleur •Bannir les logiciel contrefaits •Mises à jour automatiques •Activation et basculement sur le site de repli
Conformité et juridiques	JU	•Responsabilité civile et pénale pourrait être engagée devant les tribunaux en cas de réalisation d'un risque. Des poursuites pourraient être entamées contre la banque pour n'avoir pas procédé à une évaluation préalable et suffisante du risque et n'avoir pas mises en œuvre des mesures de protection de ses collaborateurs. •Obligations d'informations sociales •Risques de non-respect des règles prudentielles, de sécurité sanitaire, de protection des travailleurs ou de l'environnement entrainant la condamnation à une pénalité ou des actions en justice •Non-respect des règlementations imposées par les institutions financières (UEMOA, Commission bancaire)	•Poursuites judiciaires •Dégradation de l'image de la Banque •Pénalités •Fermeture de la Banque	2	3	6	3	•Respect strict de la juridiction et de la règlementation dans toute les activités •Respect strict de la juridiction dans les règlements et les embauches de la banque. •Utiliser dans la mesure du possible les règlements à l'amiable •Activation des services IT sur le site de repli
Humain	HU	•Espionnage •Actions de destruction et de sabotage •Pertes de données après une erreur de manipulation •Intrusions dans le système informatique •Mises hors service des ressources informatiques •Débauchage de salariés •Vol de supports ou de documents	•Interruption de service IT •Perte de données stratégiques	2	3	6	3	•Vérification des nouvelles recrues, prise de référence, signature d'un engagement de confidentialité, etc.. •Sauvegardes régulière des données •Limitation des habilitations d'accès à un nombre très restreint •Programme de motivation des employés pour éviter les mécontents •Programme de formation du personnel pour limiter les erreurs de manipulation •Sensibilisation

Pour chaque scénario de risque, on définit des mesures préventives et curatives pour l'atténuer, l'éviter ou le transférer. Si le risque affecte le siège dans sa globalité et menace la continuité de l'activité de la banque, le déplacement vers le site de repli doit être activé. Il nous faut pour cela déterminer les exigences en continuité d'activités.

3.2. IDENTIFICATION ET FORMALISATION DES BESOINS EN CONTINUITĒ D'ACTIVITĒ

3.2.1. Stratégie de continuité

Il s'agit de concevoir et de formaliser la stratégie de continuité conformément aux objectifs de la direction. Cette stratégie doit résulter de l'optimisation entre d'une part les exigences opérationnelles et leur coût pour respecter les objectifs de continuité, et d'autre part le coût et l'acceptabilité de l'interruption de l'activité (appréciés en fonction de la probabilité de survenue des scénarios).

On définit, dans le cadre de la stratégie, les priorités en termes de ressources et de procédures ainsi que les rôles des différents responsables pour mettre en œuvre, dans les délais prescrits, les ressources et procédures.

On doit quantifier le niveau du besoin de continuité en utilisant des indicateurs :

➔ Le niveau d'indisponibilité minimum (DMIA).

➔ Les ressources qui restent indispensables (pour la reprise d'activité).

Pour maintenir l'activité au niveau exigé par les objectifs de continuité, les processus doivent répondre à certaines attentes ou besoins.

À partir des discussions avec les responsables des métiers, nous avons pu dégager ces attentes, c'est-à-dire les services et applications qu'ils jugent nécessaires à la poursuite des activités de la banque et qu'ils utilisent dans leur travail journalier. L'effectif en ressources matérielles et humaines à secourir a aussi été déterminé.

La liste exhaustive pour tous les départements/directions est compilée dans le tableau 11 :

Tableau 11 : Besoins par service.

DEPARTEMENT	LISTE DES SERVICES DANS LE DEPARTEMENT	LISTE DES SERVICES ET APPLICATIONS A SECOURIR	EFFECTIF A SECOURIR
INFORMATION TECHNOLOGY	Support	Assistance aux utilisateurs	3
INFORMATION TECHNOLOGY	Exploitation Informatique	Compensation RTGS Applications digitales Sauvegardes Mise à jour des Bases de données WORC Dépassement / confirmation	
INFORMATION TECHNOLOGY	Réseau Télécom et sécurité	Tâches de basculement Mise à jour des tables de routage Mise à jour des règles	
TRESORERIE	Liquidité	SAGETIL ORION Dossier de partage	2
TRESORERIE	Sales	SAGETIL ORION Dossier de partage	
DIRECTION JURIDIQUE ET GOUVERNANCE	Direction	Internet Documents physiques (CR conventions, contrats, registres, etc..) ; impossibles à récupérer en cas de sinistre, à moins de tout numériser et de sauvegarder sur un serveur.	1
DIRECTION JURIDIQUE ET GOUVERNANCE	Agents		
DIRECTION FINANCIERE ET COMPTABLE	Service Comptabilité	États comptables Dossiers de partage ORION Internet	4
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle de Gestion	États comptables Dossiers de partage ORION Internet	
DIRECTION FINANCIERE ET COMPTABLE	Service Rapprochement	États comptables Dossiers de partage ORION Internet	
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle Comptable	États comptables Dossiers de partage ORION Internet	
DIRECTION DES RESSOURCES HUMAINES	Direction	AFRI-PAIE Internet Outlook	1
DIRECTION DES RESSOURCES HUMAINES	Service Gestion Prévisionnelle des Emplois	AFRI-PAIE Internet	

		Outlook	
DIRECTION DES RESSOURCES HUMAINES	Service Administration et paie	AFRI-PAIE Internet Outlook	
ORGANISATION ET QUALITE	Service Organisation	Dossier de partage Internet et VPN	1
ORGANISATION ET QUALITE	Service Qualité	Dossier de partage Internet et VPN	
COMMUNICATIONS	Service Communications	Internet	1
DIRECTION DES OPERATIONS BANCAIRES	Directeur des Opérations	Internet ORION SWIFT RTGS	7
DIRECTION DES OPERATIONS BANCAIRES	Service Étranger	Dossier de partage Internet ORION SWIFT RTGS Dépassement/Confirmation	
DIRECTION DES OPERATIONS BANCAIRES	Service Back Office Monétique	Dossier de partage Internet ORION Powercard	
DIRECTION DES OPERATIONS BANCAIRES	Service Portefeuille	Dossier de partage Internet ORION ACS RTGS CIP Dépassement/Confirmation	
DIRECTION DES OPERATIONS BANCAIRES	Service Contrôle des Opérations	Justificatifs des opérations comptables à vérifier (qui sont des supports physiques) Une solution serait de les numériser dès réception.	
DIRECTION DES OPERATIONS BANCAIRES	Caisse	Secourir quelques agences (Créer un lien avec le site backup) pour rediriger les activités de caisse, vente de produits, transfert d'argent…etc.	
DIRECTION RISQUE ET CONTRÔLE	Directeur Risque et Contrôle	Internet Siron embargo Siron AML Siron KYC ORION EFRONT	5
DIRECTION RISQUE ET CONTRÔLE	Service Contrôle Permanent	Internet ORION EFRONT WORC CIP ACS	

DIRECTION RISQUE ET CONTRÔLE	Service Conformité	Internet Siron embargo Siron AML Siron KYC CRP ORION	
DIRECTION RISQUE ET CONTRÔLE	Risque Management	Internet ORION EFRONT	
DIRECTION BANQUE DE L'ENTREPRISE	Directeur BE	Internet ORION EFRONT Dépassement/Confirmation Pricer	5
DIRECTION BANQUE DE L'ENTREPRISE	Service Grandes Entreprises	Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements	
DIRECTION BANQUE DE L'ENTREPRISE	Service Institutionnels États et démembrements	Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements	
DIRECTION BANQUE DE L'ENTREPRISE	Service Local Corporate PME - PMI	Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements	
DIRECTION BANQUE DE L'ENTREPRISE	Service Cash Management & Trade	Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements	
SERVICE LOGISTIQUES ET IMMOBILISATION	Chef Service	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	6
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Logistique	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Immobilisation	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Sécurité	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	

SERVICE LOGISTIQUES ET IMMOBILISATION	Section Archives	N/A	
DIRECTION AUDIT INTERNE	Audit Interne	Internet Dossier de partage Informations détenues sur les ordinateurs portables ; Documents des audités principalement physiques ; impossibles à récupérer en cas de sinistre. Une solution serait de les numériser dès réception.	1
DIRECTION ENGAGEMENTS	Directeur	Internet ORION Dépassement/Confirmation Dossier de partage	5
DIRECTION ENGAGEMENTS	Service Administration des engagements	Internet ORION Dépassement/Confirmation Dossier de partage	
DIRECTION ENGAGEMENTS	Service Contre-étude ou Analyse de Crédit	Internet ORION Dépassement/Confirmation Dossier de partage	
DIRECTION ENGAGEMENTS	Service Surveillance des engagements	Internet ORION Dépassement/Confirmation Dossier de partage	
DIRECTION ENGAGEMENTS	Service Recouvrement	N/A	
DIRECTION BANQUE DE DETAIL	Service Produits	N/A	1
DIRECTION BANQUE DE DETAIL	Agences	N/A	
DIRECTION BANQUE DE DETAIL	Gestionnaires de comptes	N/A	

Les services et applications nécessaires à la poursuite des activités de la banque ont ainsi été déterminés. Il faut à présent matérialiser l'effectif en ressources humaines et physiques à secourir.

3.2.2. Besoins de continuité pour les ressources critiques

Il est question ici de formaliser les objectifs de disponibilité pour les infrastructures (bâtiments, locaux), les systèmes d'information et les ressources humaines (équipes, personnel clés, compétences).

L'effectif en ressources matérielles et humaines à mettre en place sur le site de secours a été évalué pour chaque métier. Une compilation est donnée dans le tableau 12.

Tableau 12: Effectifs en ressources humaines à secourir et nombre de machines associées.

DEPARTEMENT	EFFECTIF EN SITUATION NORMALE	EFFECTIF A SECOURIR	% SECOURU	LAPTOP/ DESKTOP	EMPLACEMENT
COMMUNICATIONS	1	1	100%	1	Télétravail
DIRECTION AUDIT INTERNE	3	1	33%	1	Télétravail
DIRECTION BANQUE DE DETAIL	2	2	100%	2 desktops	Site de repli
DIRECTION BANQUE DE L'ENTREPRISE	12	5	42%	5	Télétravail
DIRECTION DES OPERATIONS BANCAIRES	17	7	41%	0+6 desktops	Site de repli
DIRECTION DES RESSOURCES HUMAINES	3	1	33%	1	Télétravail
DIRECTION ENGAGEMENTS	10	5	50%	2+3 desktops	2 en Télétravail ; 3 sur le site de repli
DIRECTION FINANCIERE ET COMPTABLE	8	4	50%	4	Télétravail
DIRECTION JURIDIQUE ET GOUVERNANCE	3	1	33%	1	Télétravail
DIRECTION RISQUE ET CONTRÔLE	8	5	63%	4+1 desktop	4 en Télétravail ; 1 sur le site de repli
INFORMATION TECHNOLOGY	4	3	75%	0+3 desktops	Site de repli
ORGANISATION ET QUALITE	3	1	33%	1	Télétravail
SERVICE LOGISTIQUES ET IMMOBILISATION	20	6	30%	1	Télétravail
TRESORERIE	3	2	67%	0+2 desktops	Site de repli
DIRECTION GENERALE	2	1	50%	1	Télétravail
Total	**99**	**45**	**45%**	**22 Laptops+17 Desktops**	

La DMIA (Durée maximale d'interruption admise) a été évaluée par la direction Risques et Contrôles pour certains processus critiques de la banque. Elle est résumée dans le tableau 13.

Tableau 13 : DMIA pour les services critiques et besoins secours métiers.

DEPARTEMENT	LISTE DES SERVICES DANS LE DEPARTEMENT	EFFECTIF A SECOURIR	ACTIVITES	LISTE DES SERVICES ET APPLICATIONS A SECOURIR	PROCESSUS	DMIA
INFORMATION TECHNOLOGY	Support	2	• Support aux utilisateurs • Traitement de la compensation • Suivi du fonctionnement RTGS • Suivi de la gestion des applications digitales • Restauration des sauvegardes • Mise à jour des Bases de données • Traitement des applications de crédit (WORC) • Traitement des applications de dépassement/confirmation • Gestion du réseau de la banque • Tâches de basculement • Mise à jour des tables de routage • Mise à jour des règles	N/A	N/A	Variable
INFORMATION TECHNOLOGY	Exploitation Informatique			Compensation RTGS Applications digitales Sauvegardes Mise à jour des Bases de données WORC Dépassement / confirmation	**Processus de la gestion de la compensation** : IT-Opérations-BCEAO-ABI **Processus de la gestion de RTGS :** Opérations -IT - ABI - BCEAO	24H
INFORMATION TECHNOLOGY	Réseau Télécom et sécurité			Tâches de basculement Mise à jour des tables de routage Mise à jour des règles	**Processus Gestion de la disponibilité des Plateformes** : ABI – IT – Agences/Services - Utilisateur	24H
TRESORERIE	Liquidité	2	•Transferts (Achat, vente de devises) •Emprunts •Placements (Titres, obligations)	SAGETIL ORION Dossier de partage	**Processus de TRANSFERTS :** Client-Réception-Service étranger-gestionnaire-Trésorerie-Service étranger. **Processus d'Emprunts :** RTGS-SAGETIL-Dépôt manuel **Processus de Placements :** RTGS-SAGETIL	24H
TRESORERIE	Sales			SAGETIL ORION Dossier de partage		

DIRECTION JURIDIQUE ET GOUVERNANCE	Direction	1	•Conventions •Contrats •Garanties	Internet Documents physiques (CR conventions, contrats, registres, etc..) ; impossibles à récupérer en cas de sinistre, à moins de tout numériser et de sauvegarder sur un serveur.	N/A	
DIRECTION JURIDIQUE ET GOUVERNANCE	Agents	N/A				
DIRECTION FINANCIERE ET COMPTABLE	Service Comptabilité	4	•Ordonnancement des dépenses •Règlement des dépenses •Factures •Rapports •Rapports à la BCEAO	États comptables Dossiers de partage ORION Internet	**Processus d'Ordonnancement des dépenses** : Moyens Généraux - Gestion financière - Direction Générale. **Processus de règlement des dépenses :** Moyens Généraux - DFC - DO - DG - DO	
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle de Gestion			États comptables Dossiers de partage ORION Internet	N/A	
DIRECTION FINANCIERE ET COMPTABLE	Service Rapprochement			États comptables Dossiers de partage ORION Internet	N/A	
DIRECTION FINANCIERE ET COMPTABLE	Service Contrôle Comptable			États comptables Dossiers de partage ORION Internet	N/A	
DIRECTION DES RESSOURCES HUMAINES	Service Gestion Prévisionnelle des Emplois	1	•Gestion prévisionnelle des emplois •Recrutements •Formations •Communication interne •Gestion des évaluations	Outlook AFRI-PAIE Internet	N/A	

			des performances du personnel •Élaboration de rapports RH (Bilan social, activités)			
DIRECTION DES RESSOURCES HUMAINES	Service Administration et paie		•Gestion administrative •Paiement des salaires •Paiement des taxes •Cotisations CNSS •Prise en charge Santé	Outlook AFRI-PAIE Internet	N/A	
ORGANISATION ET QUALITE	Service Organisation	1	•Gestion des projets SI •Mise en œuvre •Maintenance •Paramétrage des systèmes •Assistance aux utilisateurs •Gestion et suivi des réclamations	Dossier de partage Internet et VPN	N/A	3 JOURS
ORGANISATION ET QUALITE	Service Qualité			Dossier de partage Internet et VPN	N/A	
COMMUNICATIONS	Service Communications	1	•Gestion des communications de la Banque	Internet	N/A	
DIRECTION DES OPERATIONS BANCAIRES	Service Étranger	6	•Transferts •CREDOC import-export •REMDOC import-export •Suivi règlementation (R08) •Back office TRESO •Rapports BCEAO, Ministère des finances	Dossier de partage Internet ORION SWIFT RTGS Dépassement/Confirmation	**PROCESSUS TRANSFERT :** Réception - DO - Chef service Étranger - Agent service Étranger - Chef service Étranger - DO (pour validation finale) **PROCESSUS CREDOC :** DBE - DE - CIC (ou CSC) - BCP **PROCESSUS REMDOC** : DBE - DBD - TRESO	48H
DIRECTION DES OPERATIONS BANCAIRES	Service Back Office Monétique		•Gestion des transferts d'argent •Gestion des guichets automatiques et des cartes •Gestion des réclamations •Réconciliation des comptes monétiques •M-Banking •Réconciliation des comptes des cartes internationales	Dossier de partage Internet ORION Powercard	**PROCESSUS RECLAMATIONS** : Agence - réception/courrier - DG - DO - Monétique - agence (par courrier) **PROCESSUS TRANSFERTS :** Agents commerciaux - Front office - Gestionnaire de transfert rapide	1 SEMAINE

					Gestion des guichets automatiques : Charges de clientèle - Service BO Monétique **PROCESSUS M-BANQUING** : MOOV - R.O. Qualité - Gestionnaire de transfert rapide	
DIRECTION DES OPERATIONS BANCAIRES	Service Portefeuille		•Réception et dispatching de tous les ordres (Virements, chèques, etc..) •Gestion des virements •Gestion des chèques •Génération des fichiers salaires •1ere et 2eme Validation portefeuille local •Dépouillement et dispatching des messages RTGS et SWIFT	Dossier de partage Internet ORION ACS RTGS CIP Dépassement/Confirmation	**PROCESSUS VIREMENTS :** Réception - DO - Chef Service Portefeuille ou DO (selon le montant pour validation) **PROCESSUS CHEQUES :** Réception par l'agent clientèle/mail/agence/poste/bornes - agent Service Portefeuille (pour traitement) **PROCESSUS Validation portefeuille local** : Monétique - Service Étranger - CAD - Caisse	72H
DIRECTION DES OPERATIONS BANCAIRES	Service Contrôle des Opérations	N/A	•Vérification des Operations comptables	Justificatifs des opérations comptables à vérifier (qui sont des supports physiques) Une solution serait de les numériser dès réception.	N/A	
DIRECTION DES OPERATIONS BANCAIRES	Caisse	0	•Opérations de dépôts •Opérations de retraits •Opérations de Transfert d'argent •Achat et vente de devises	Secourir quelques agences (créer un lien avec le site backup) pour rediriger les activités de caisse, vente de produits, transfert d'argent…etc.	N/A	24H

DIRECTION RISQUE ET CONTRÔLE	Directeur Risque et Contrôle	N/A		Internet Siron embargo Siron AML Siron KYC ORION EFRONT	N/A	
DIRECTION RISQUE ET CONTRÔLE	Service Contrôle Permanent	3	•Contrôle •Détection et enregistrement des incidents	Internet ORION EFRONT WORC CIP ACS	N/A	
DIRECTION RISQUE ET CONTRÔLE	Service Conformité	1	•Gestion de la conformité •Réquisitions •Profilage et filtrage de la clientèle •Filtrage des transactions	Internet Siron embargo Siron AML Siron KYC CRP ORION	**PROCESSUS Courrier de réponse ou réquisition venant de CENTIF :** Réception courrier - DG - DRC - Service conformité - DRC - Transmission à la CENTIF **PROCESSUS REQUETE** Correspondant bancaire : DO (pour réception) - Charge de clientèle (pour traitement) - DO - Service Conformité (pour vérification physique des informations données) - DRC (pour validation) - Service Conformité - DO (pour transmission)	
DIRECTION RISQUE ET CONTRÔLE	Risque Management	1	•Déclaration et collecte des incidents •Validation de la cartographie des risques •Gestion des risques	Internet ORION EFRONT	**PROCESSUS Déclaration et collecte des incidents :** Contrôle Permanent (Pour détection et enregistrement) - Risques (Pour validation et mise à jour de la cartographie des risques)	
DIRECTION BANQUE DE L'ENTREPRISE	Directeur BE	1		Internet ORION EFRONT Dépassement/Con	N/A	

				firmation Pricer		
DIRECTION BANQUE DE L'ENTREPRISE	Service Grandes Entreprises	4	•Gestion des dépassements •Confirmation •Crédit aux entreprises •Prospection des clients •Développement de la relation client •Montage de dossier de crédit aux entreprises •CREDOC/REMDOC aux entreprises	Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements	**PROCESSUS DE DEPASSEMENT :** Caisse ou agent des Opérations = initiateur - Gestionnaire - DBE/DBD - DE (Risques) - CAD (Contrôle admin du crédit - caisse ou agent des Opérations = initiateur) **PROCESSUS DE CONFIRMATION :** Caisse ou agent des Opérations = initiateur - Gestionnaire - initiateur	24H
DIRECTION BANQUE DE L'ENTREPRISE	Service Institutionnels États et démembrements			Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements		48H
DIRECTION BANQUE DE L'ENTREPRISE	Service Local Corporate PME - PMI			Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements		24H
DIRECTION BANQUE DE L'ENTREPRISE	Service Cash Management & Trade			Internet ORION Dépassement/Confirmation Pricer Secourir quelques agences pour les paiements		24H
SERVICE LOGISTIQUES ET IMMOBILISATION	Chef Service	1		Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	N/A	

SERVICE LOGISTIQUES ET IMMOBILISATION	Section Logistique	3	•Gestion de la logistique •Achats •Bons de commande •Gestion des fournisseurs	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	**PROCESSUS ACHATS:** Service demandeur (expression du besoin) - SLI (pour initier l'achat) - Fournisseur (pour les factures pro-forma) - Contrôleur de gestion (pour l'imputation dans l'application budgétaire) - Impression - Chargé des achats - Chef SLI - Contrôleur de gestion - DFC- DO - DG - SLI (pour le bon de commande) - Chargé des achats - Chef SLI - DO - DFC - DG - fournisseur (pour la livraison) - SLI - fournisseur (pour dépôt de facture) - SLI (pour paiement) - Comptabilité - DFC - DO - DG - Comptabilité - DO (pour saisie dans Orion)	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Immobilisation	1		Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage		
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Sécurité	1	•Gestion de la Sécurité physique	Internet IMMOTECH IMPUTATION BUDGETAIRE Dossier de partage	**PROCESSUS GESTION DES ACCES :** Départements - SLI	
SERVICE LOGISTIQUES ET IMMOBILISATION	Section Archives	N/A	•Archivage des documents de la Banque	N/A	N/A	

DIRECTION AUDIT INTERNE	Direction Audit Interne	1	•Audits interne	Internet Dossier de partage Informations détenues sur les ordinateurs portables ; Documents des audités principalement physiques ; impossibles à récupérer en cas de sinistre. Une solution serait de les numériser dès réception.	N/A	
DIRECTION ENGAGEMENTS	Directeur	1		Internet ORION Dépassement/Confirmation Dossier de partage	N/A	
DIRECTION ENGAGEMENTS	Service Administration des engagements	2	•Gestion administrative des engagements •Suivi des créances en souffrance non contentieuses •Analyse des crédits •Gestion de l'état des engagements conformément aux contrats •Rapports aux autorités monétaires •Rapports statistiques périodiques d'engagement de crédit •Recouvrements	Internet ORION Dépassement/Confirmation Dossier de partage	**PROCESSUS OCTROI DE CREDIT** : Commercial - DE (pour la contre étude) - Comité de Crédit (DG, DBE, DBD, DE) - Gestionnaire - Client - DJG - Administration des engagements (pour introduction dans le système et mise en place) - DO (pour validation)	
DIRECTION ENGAGEMENTS	Service Contre-étude ou Analyse de Crédit	1		Internet ORION Dépassement/Confirmation Dossier de partage		72H
DIRECTION ENGAGEMENTS	Service Surveillance des engagements	1		Internet ORION Dépassement/Confirmation Dossier de partage		
DIRECTION ENGAGEMENTS	Service Recouvrement	N/A		N/A		

DIRECTION BANQUE DE DETAIL	Service Produits	Quelques agences à connecter avec le site secours pour y rediriger les activités de caisse	•Vente des produits de la banque : Offres packagées, Cartes, Épargnes et classement, Bancassurance, transfert d'argent •Assistance clientèle	N/A	N/A	
DIRECTION BANQUE DE DETAIL	Agences			N/A	N/A	
DIRECTION BANQUE DE DETAIL	Gestionnaires de comptes			N/A	N/A	

Légende

"Limité" entre 7 et 10
"Important" entre 11 et 13
"Grave" entre 14 et 16
"Critique" entre 17 et 20

DMIA: Durée Maximale d'Interruption Admissible
BIA: Business Impact Analysis

Après avoir formalisé les besoins en continuité du métier, c'est-à-dire les applications, les ressources humaines, les outils de travail, etc., la continuité des plateformes sur lesquelles tournent ces activités doit aussi être maintenue. D'où la nécessité d'analyser l'architecture du réseau de la BATG afin de définir sa continuité.

3.3. ARCHITECTURE RĒSEAU TYPE A METTRE EN ŒUVRE DANS LE CADRE DU PCA D'UNE FILIALE DU GROUPE ABI

La figure 8 présente l'architecture réseau type à mettre en œuvre dans le cadre du plan de continuité d'activités d'une filiale du groupe ABI.

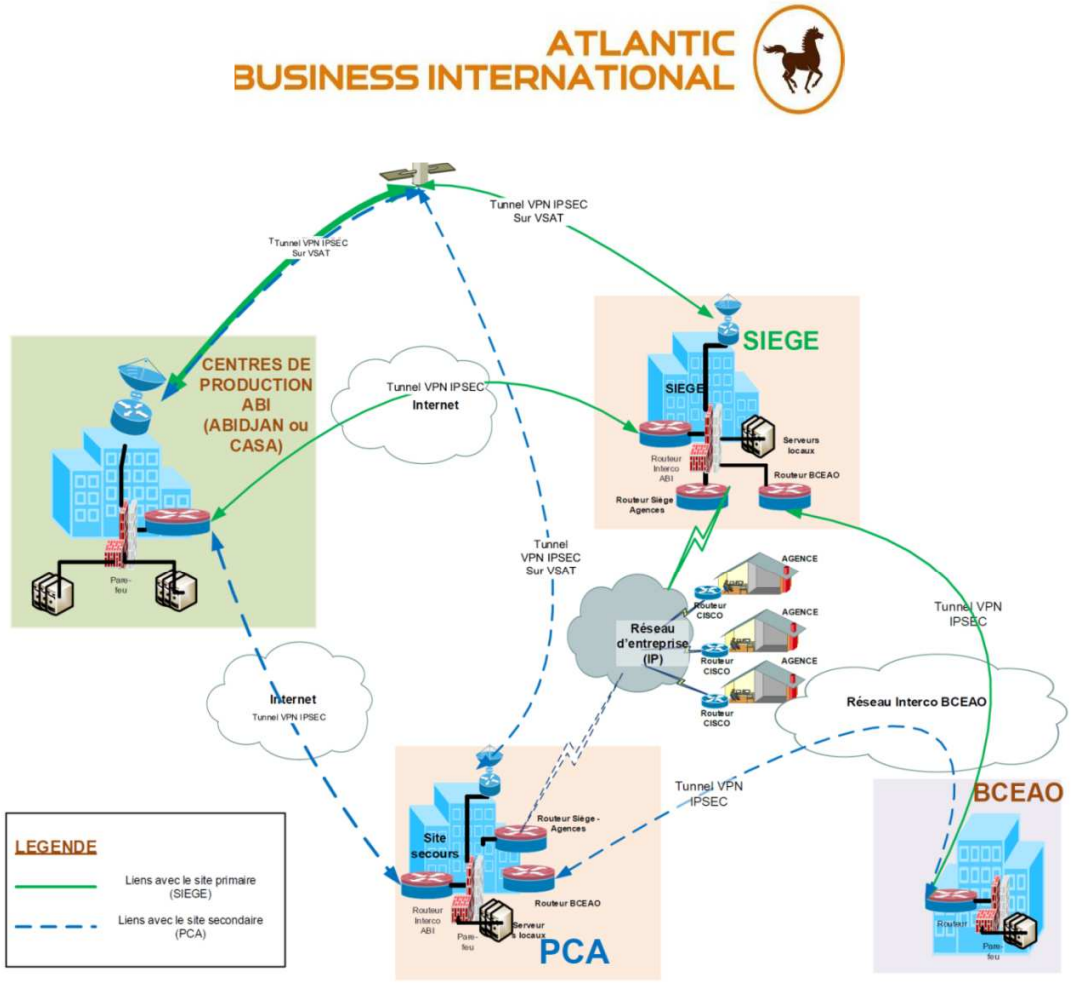


Figure 8 : Schéma d'architecture type du groupe ABI.

3.3.1. En situation normale

En situation normale, le fonctionnement est comme suit :

➔ Les filiales sont connectées au centre de production d'ABI d'Abidjan et de Casablanca par VPN au moyen de la VSAT et d'Internet. Elles sont aussi connectées à la BCEAO par tunnel VPN, aux agences et au site de secours (Site PCA).

- ➔ Le site de secours existant de la BATG est aussi relié aux sites de productions d'ABI par Internet avec une connexion et un débit en adéquation avec le volume de données à répliquer. Il devrait aussi être connecté par VSAT, mais cette dernière n'est pas déployée pour le moment.
- ➔ Les agences et les sites distants passent par le siège de la filiale pour toutes communications avec les Datacenter d'ABI (Abidjan et Casablanca). Elles devraient aussi idéalement être reliées au site PCA.
- ➔ Les opérations de télé-compensation sont réalisées au siège directement connecté à la BCEAO.
- ➔ La BCEAO est aussi reliée au site PCA.

3.3.2. En mode PCA

En mode PCA, c'est-à-dire en cas de crise ou d'indisponibilité du siège, le site secours prend le relais et sert de Hub pour les activités critiques de la Banque.

- ➔ Les agences et sites distants passent par le site PCA pour toutes communications avec les Datacenter d'ABI.
- ➔ Les opérations de télé-compensation sont réalisées depuis le site PCA qui est directement connecté avec la BCEAO.
- ➔ Afin de s'assurer de la disponibilité des communications entre les agences et les Datacenter d'ABI via le site PCA, quelques agences devraient être connectées de façon permanente aux sites de production d'Abidjan et de Casablanca via le site PCA.
- ➔ Dans le présent plan, nous avons prévu de secourir 6 agences. Elles seront de ce fait planifiées pour être connectées au site PCA.

3.3.3. Cas de BATG

3.3.3.1. En situation normale

En situation normale, idéalement, l'architecture réseau de la BATG est schématisée comme dans la figure 9 :

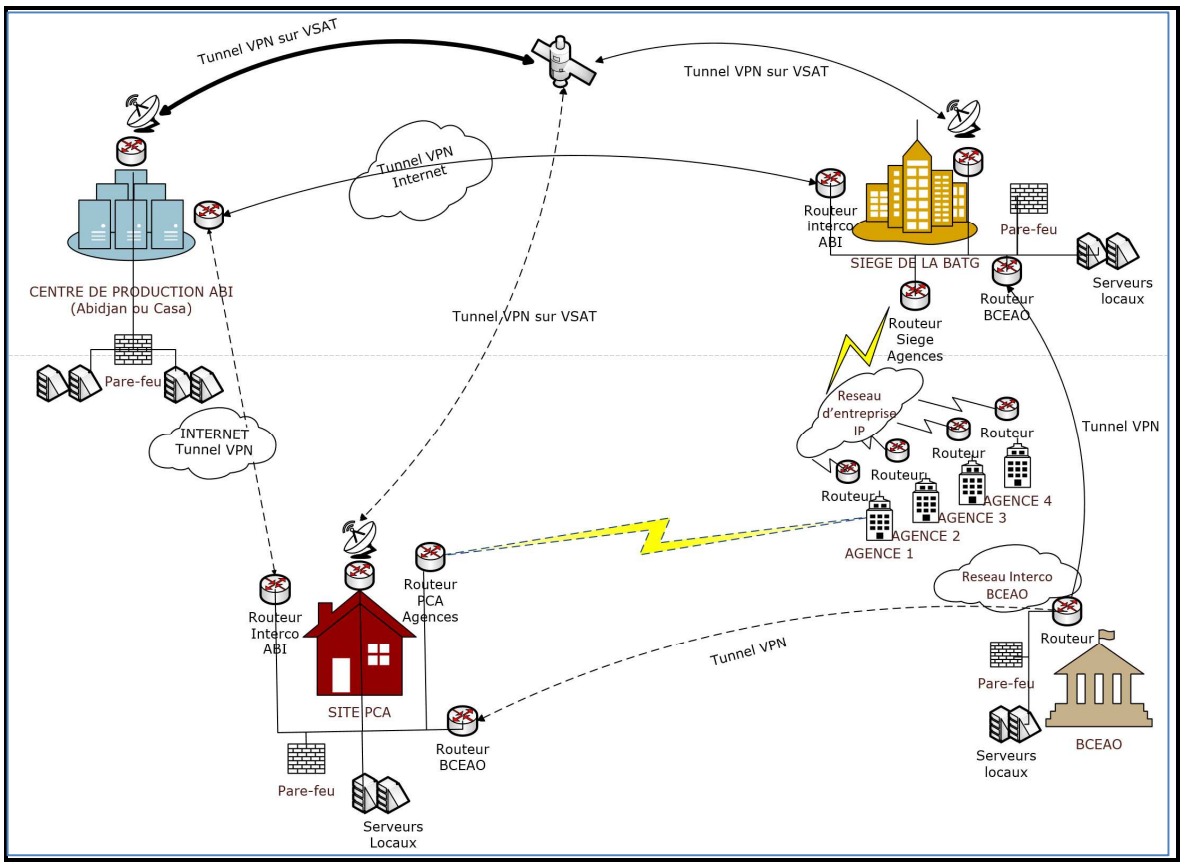


Figure 9 : Schéma d'architecture de la BATG.

3.3.3.2. En mode PCA

Dans le cas d'un sinistre grave affectant le siège de la filiale, l'architecture réseau de la BATG devient telle qu'elle est schématisée dans la figure 10 :

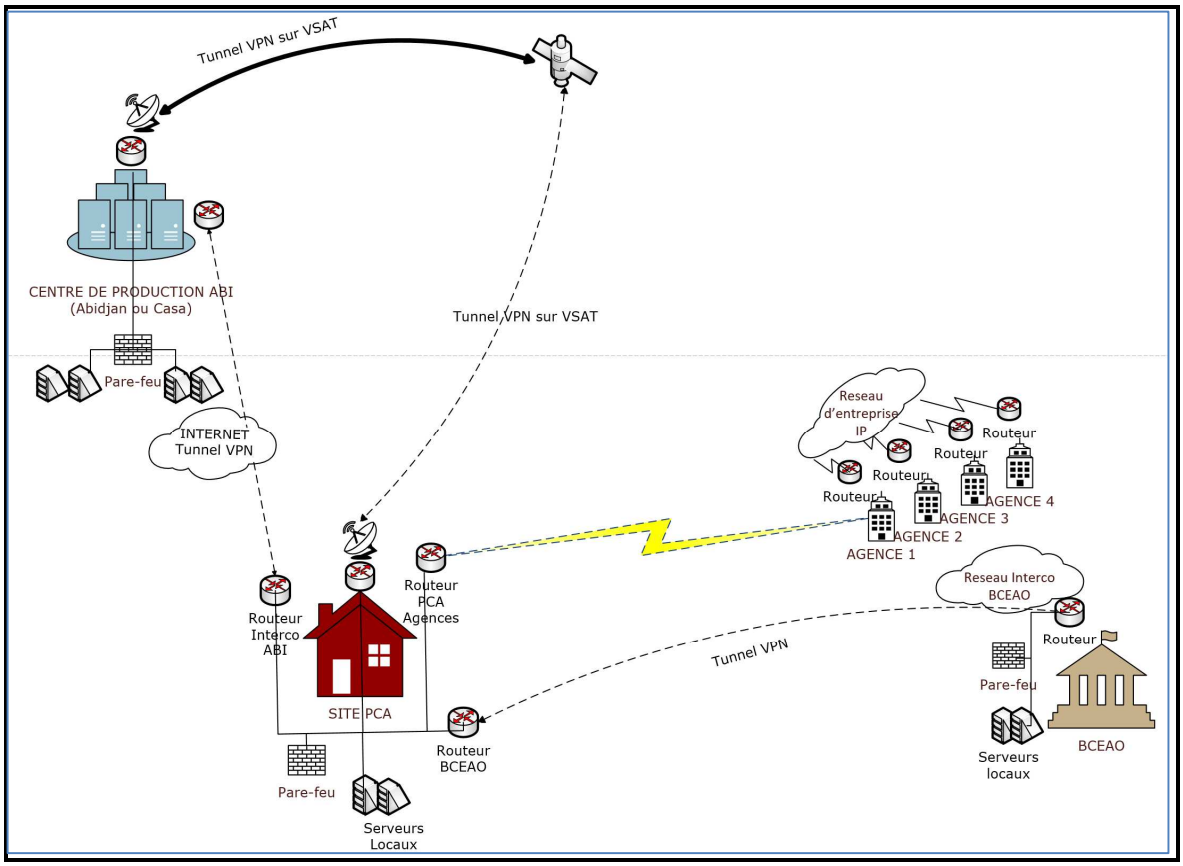


Figure 10 : Schéma d'architecture type pour BATG en mode PCA.

En résumé, en cas de sinistre, la nouvelle architecture du réseau est telle que le site de repli prend la place du siège et devient le centre de production temporaire. Les agences secourues y seront redirigées. C'est pourquoi le site PCA doit être choisi avec soin et remplir les exigences répondant aux normes internationales.

3.4. CHOIX DU SITE DE REPLI

3.4.1. Conditions d'implantation

Le choix d'un site de repli est une étape vitale pour la mise en condition opérationnelle du PCA.

Ce site devra répondre à un besoin d'accueil de ressources humaines, matérielles et logicielles en cas d'indisponibilité totale ou partielle, ou en cas de difficultés d'accès au siège.

La sélection du site de secours répondant aux exigences techniques, sécuritaires et métier permettra de redémarrer les activités critiques de la banque dans des conditions optimales, dans la mesure où il devra abriter aussi bien toute l'infrastructure technique, que les ressources nécessaires qui assureront la continuité de l'activité.

- ➔ Le site doit être suffisamment distant du site principal (minimum 80 km à titre indicatif, d'après les recommandations d'ABI).
- ➔ Il ne doit pas se situer dans une zone inondable, ni au bord de la mer ou d'un cours d'eau.
- ➔ Il ne doit pas être dans une zone de forte habitation ni là où il y a des risques de feux de forêts.
- ➔ Il doit être distant d'au moins 30 km de l'aéroport (à titre indicatif, d'après les recommandations d'ABI), d'usines, de grands centres commerciaux, de ponts ou barrages.
- ➔ Il doit être placé au rez-de-chaussée pour en faciliter l'accès.
- ➔ Il doit offrir un espace de travail temporaire suffisamment grand pour accueillir le personnel secouru.
- ➔ Il doit avoir un groupe électrogène de grande autonomie (48h au moins) afin de pallier aux cas de coupures électriques de longue durée, une réserve de carburant conséquente, ainsi qu'un onduleur. Les installations doivent être conformes aux normes en vigueur (parafoudre, paratonnerre, mise à la terre, etc.).
- ➔ L'interconnexion réseau entre le site de secours et le site principal doit être redondée par une liaison de secours acheminée sur un parcours différent de celui de la liaison principale et fournie par un prestataire différent également.
- ➔ Les équipements du cœur du réseau (Switch, routeurs, …) doivent être redondés.
- ➔ Les normes de sécurité usuelles doivent être respectées sur le site (Vidéo surveillance, alarmes incendie, intrusion, extinction automatique, aération, étanchéité, portes coupe-feu, etc.).

- ➔ Le système de contrôle d'accès doit être restreint et automatisé par des badges, des PIN ou biométrique.
- ➔ Le site ne doit pas avoir d'accès donnant sur une zone non contrôlée.
- ➔ Il doit disposer de protections périmétriques adéquates comme des murs surélevés, opaques et solides, un blindage selon le risque local, une solidité, une limitation du nombre de portes, etc.

Le site de repli pour le cas de notre étude, doit pouvoir contenir les effectifs définis en [3.2.2] et explicités dans le tableau 14 :

Tableau 14 : Effectifs du site de Repli.

DEPARTEMENT	EFFECTIF EN SITUATION NORMALE	EFFECTIF A SECOURIR	% Secouru	EMPLACEMENT	Laptop (Télétravail)	Ordinateur de bureau	Table de bureau	Fauteuil de bureau	Imprimante	Téléphone fixe	Scanneur	Cachet
COMMUNICATIONS	1	1	100%	Télétravail	1	0	0	0	0	0	0	0
DIRECTION AUDIT INTERNE	3	1	33%	Télétravail	1	0	0	0	0	0	0	0
DIRECTION BANQUE DE DETAIL	2	2	100%	Site de repli	0	2	2	2	0	0	0	0
DIRECTION BANQUE DE L'ENTREPRISE	12	5	42%	Site de repli	5	0	0	0	0	0	0	0
DIRECTION DES OPERATIONS BANCAIRES	17	7	41%	Site de repli	0	6	6	6	1	0	1	2
DIRECTION DES RESSOURCES HUMAINES	3	1	33%	Télétravail	1	0	0	0	0	0	0	0
DIRECTION ENGAGEMENTS	10	5	50%	2 en Télétravail 3 sur Site de repli	2	3	3	3	0	0	0	0
DIRECTION FINANCIERE ET COMPTABLE	8	4	50%	Télétravail	4	0	0	0	0	0	0	0
DIRECTION JURIDIQUE ET GOUVERNANCE	3	1	33%	Télétravail	1	0	0	0	0	0	0	0
DIRECTION RISQUE ET CONTRÔLE	8	5	63%	4 en Télétravail 1 sur Site de repli	4	1	1	1	0	0	0	0
IT	4	3	75%	Site de repli	0	3	3	3	0	1	0	0
ORGANISATION ET QUALITE	3	1	33%	Télétravail	1	0	0	0	0	0	0	0
SERVICE LOGISTIQUES ET IMMOBILISATION	20	6	30%	Télétravail	1	0	0	0	0	0	0	1
TRESORERIE	3	2	67%	Site de repli	0	2	2	2	1	0	0	0
DG	2	1	50%	Télétravail	1	0	0	0	0	0	0	0
TOTAL	**99**	**45**	**45%**		**22**	**17**	**17**	**17**	**2**	**1**	**1**	**3**

En plus de remplir les exigences liées à l'effectif, le site de secours doit :

- ➔ Avoir un accès simplifié mais aussi s'éloigner de Lomé ou du siège.
- ➔ Avoir au moins deux voies d'accès à la localité, bitumées ou non mais praticable même en période de pluies.
- ➔ Se trouver dans une localité assez grande, lotie, assainie, et ayant une disponibilité de liaisons à haut débit pour la reprise de l'activité.
- ➔ Avoir des accès faciles aux Télécoms pour le déploiement des infrastructures afin de reconnecter un certain nombre d'agences du réseau (IP, MPLS ou BLR).
- ➔ Respecter les recommandations de sécurité pour permettre le bon déroulement de la stratégie de continuité.

Pour recevoir cet effectif, le site doit avoir approximativement les dimensions ci-dessous :

D'après [10] Office Space Planning Standards, l'espace nécessaire pour aménager un bureau est d'environ 6,7 m².

Pour 13 ordinateurs et 13 bureaux, nous aurons besoin de 87.1 m². À cela Il faut y ajouter :

- ➔ Une salle serveur, d'une superficie d'environ 20 m².
- ➔ Une salle d'énergie pour les coffrets électriques, les onduleurs et les régulateurs = 9 m².
- ➔ Une salle de réunion pouvant contenir jusqu'à 10 personnes = 14 m².
- ➔ Des toilettes = 8 m².
- ➔ Une salle agents d'entretien = 4.7 m².

Au total : **142.8 m²** de superficie des salles pour accueillir l'effectif du site de secours.

Dans le paragraphe qui suit, nous faisons des propositions de localisations de ce site.

3.4.2. Propositions de sites

3.4.2.1. Proposition 1 :

Construire un nouveau site physique avec toutes les infrastructures nécessaires mises en place.

Option proposée 1 : KOVIE, qui se trouve à 27 km du siège (Figure 11).
Trois grandes voies (dont Route de mission Toé) non bitumées la relient à un embranchement de la Nationale 1 et au Boulevard du 30 Août.

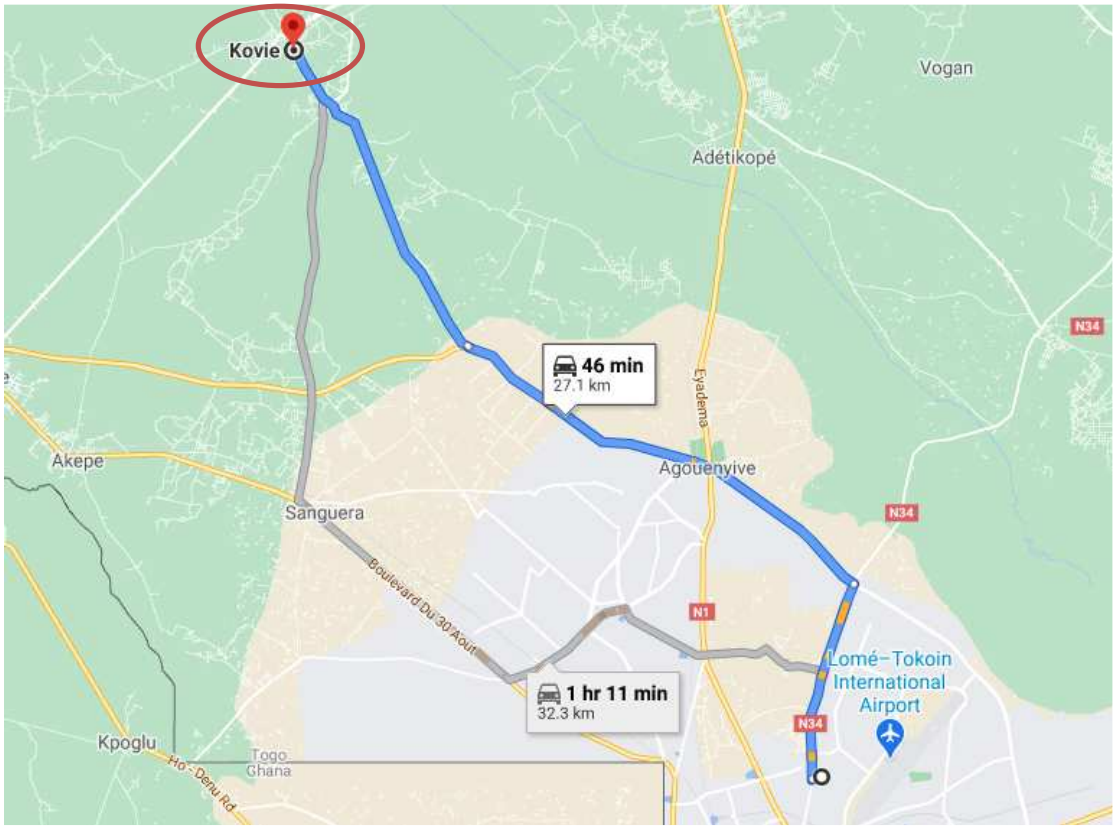


Figure 11 : Proposition Site de KOVIE.

Option proposée 2 : Proche de Marché AVETA, dans la Préfecture de Zio qui se trouve à 19 km du siège (Figure 12).
On y a accès par les Nationale 2 et 34, ainsi que 2 routes secondaires.

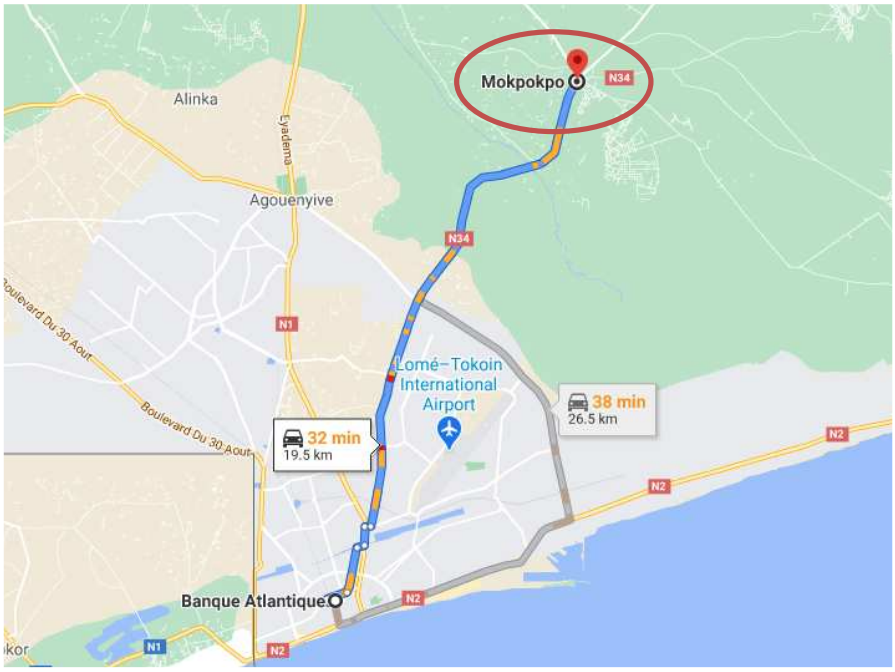


Figure 12 : Proposition site d'AVETA.

Option proposée 3 : NOEPE, qui se trouve à 28 km du siège (Figure 13)
La localité se trouve à l'intersection de deux grandes voies bitumées (dont le Boulevard du 30 Août).

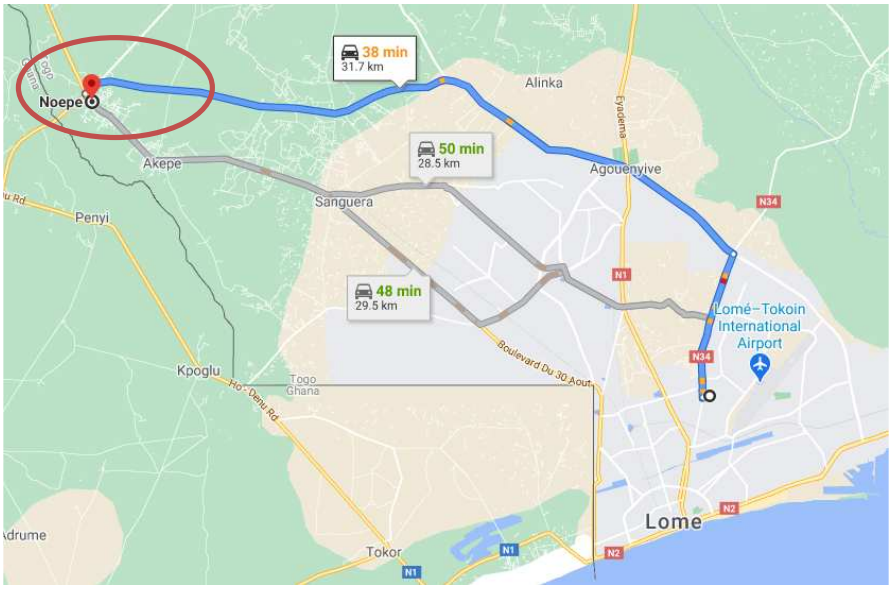


Figure 13 : Proposition site de NOEPE.

3.4.2.2. Proposition 2 :

Co-localiser avec une agence existante qui se situerait dans la périphérie de Lomé.

Dans un souci de gestion des coûts, cette proposition est un compromis intéressant par rapport à la construction d'un nouveau site de repli. La difficulté est qu'aucune agence de Lomé et périphéries ne répond aux exigences de dimensions et de sécurité requises. L'agence Banque Atlantique d'AGOE aurait pu être une possibilité mais le site est très exposé et se situe au bord de la Nationale N1.

La solution serait donc de construire une nouvelle agence dans la périphérie de Lomé en intégrant les exigences suscitées.

Le risque majeur que comporterait cette solution, est que le site se trouvant à Lomé, s'il n'est pas suffisamment éloigné du siège, pourrait aussi être indisponible en cas de catastrophe naturelle ou de mouvements sociaux dans la ville.

Cependant, cette solution présenterait aussi plusieurs avantages :

- ➔ L'agence serait accessible par au moins deux grandes voies.
- ➔ Les locaux appartiendraient déjà à la banque.
- ➔ Cela créerait de l'activité dans la zone, donc moins de risques sécuritaires ou d'attaques contrairement à un site toujours vide.
- ➔ Une extension est plus facilement envisageable.
- ➔ Les collaborateurs connaitraient déjà les locaux.
- ➔ Les évolutions / modifications seraient rapides à mettre en œuvre.
- ➔ La partie réseau et débits serait maitrisée.

Dans les Figures 14, 15 et 16, nous faisons une proposition de localisation dans une des zones périphériques de Lomé, SANGUERA :

- ➔ Le site proposé est accessible par 2 grandes voies (dont le Boulevard du 30 Août) et est distant de 22 Km environ du siège de la BATG ; Il est à 1.5 Km de la station d'essence la plus proche ; à 16 Km à vol d'oiseau de l'aéroport et à 15 Km également à vol d'oiseau de la mer.

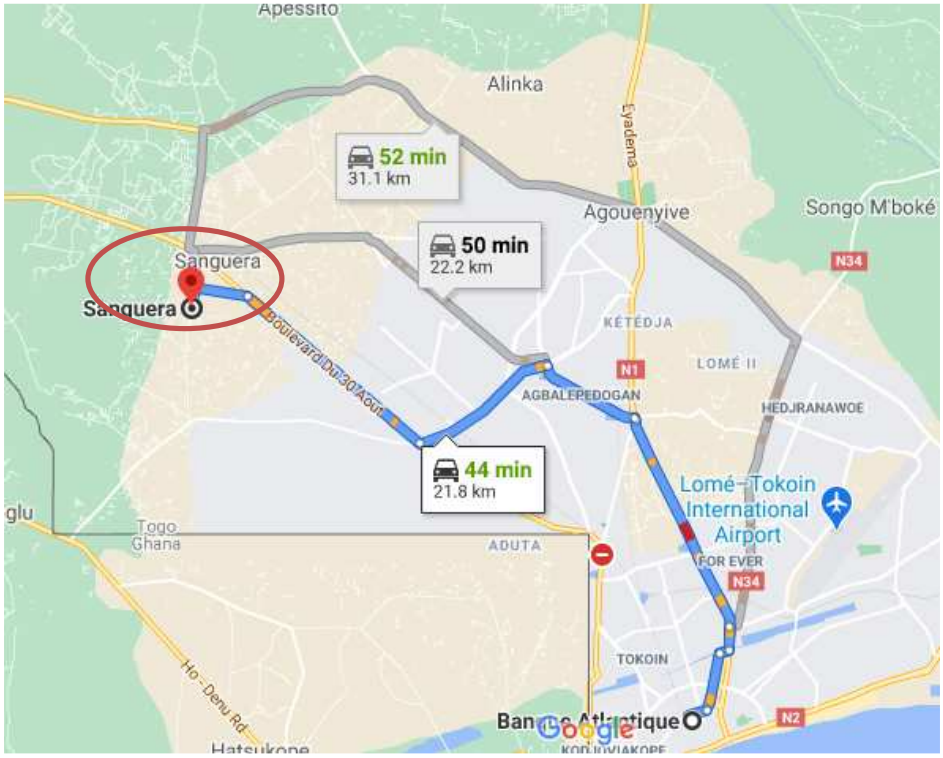


Figure 14 : Site de Sanguera.

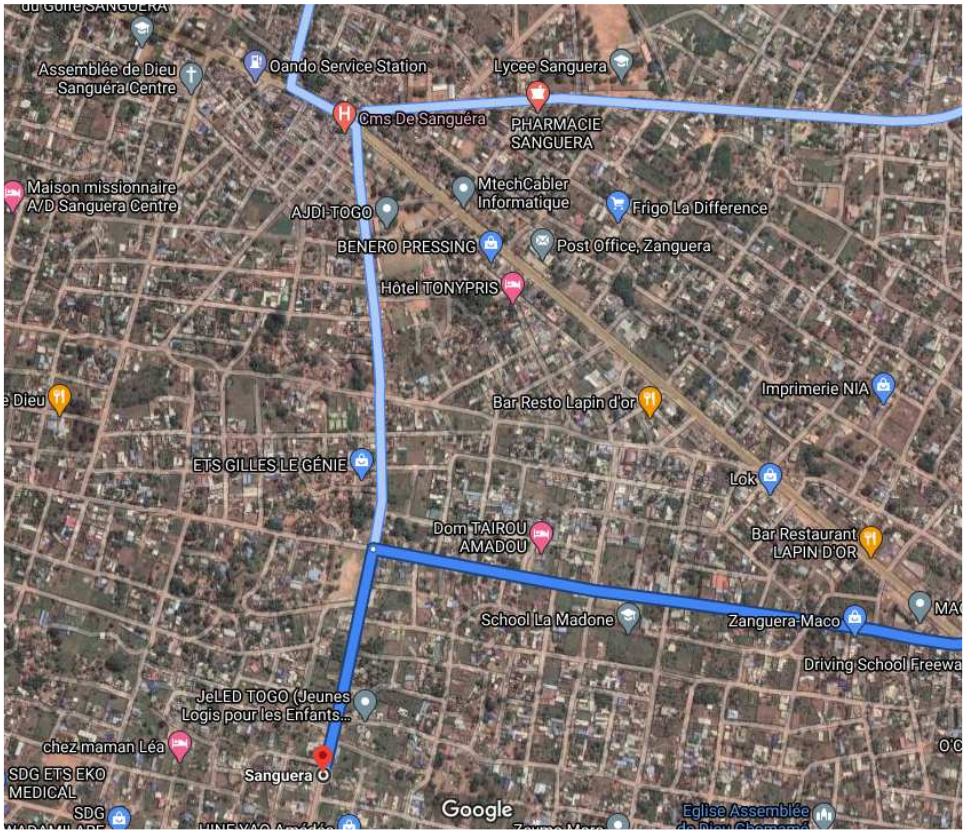


Figure 15 : Site de Sanguera, Satellite.

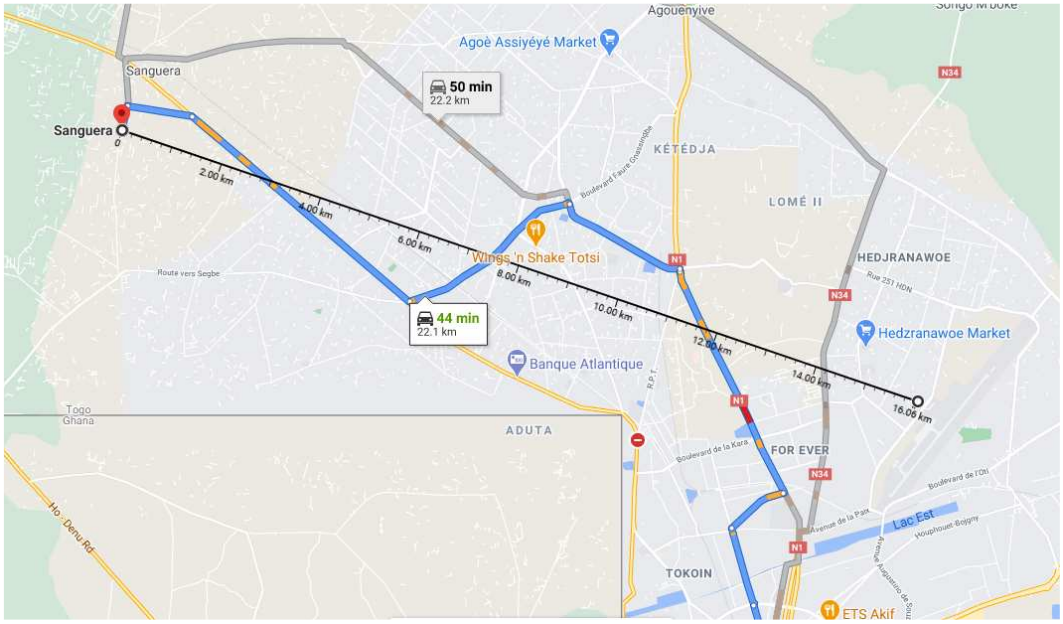


Figure 16 : Site de Sanguera, distances.

Il est cependant important de noter que tous ces sites comportent des risques inhérents entre autres à leur localisation. Dans ce contexte, nous allons procéder à l'analyse de risque de ces propositions.

3.4.2.3. Analyse de risques des propositions

En procédant à l'analyse de risques des propositions des sites de repli dans les deux cas : la construction d'un nouveau site et la colocalisation avec une nouvelle agence, il ressort les deux cartographies explicitées dans le tableau 15.

Tableau 15 : Cartographie Risques des propositions de site de repli.

					NIVEAU DE RISQUE DU SITE AVANT TRAITEMENT			NIVEAU DE RISQUE DU SITE APRES TRAITEMENT			
SITE DE REPLI	**CHOIX DU SITE**	**SITUATION**	**SCENARIO DE RISQUES**	**DESCRIPTION**	**PROBABILITE**	**IMPACT**	**NIVEAU DE RISQUE AVANT TRAITEMENT**	**Mesures préventives**	**PROBABILITE**	**IMPACT**	**NIVEAU DE RISQUE APRES TRAITEMENT**
Proposition 1	KOVIE AVETA NOEPE	•Les 3 sites ne se trouvent pas dans une zone inondable, ni à proximité de la mer ou d'un cours d'eau. •Il n'y a pas de forets environnantes •Ce n'est pas une zone de fortes habitations, ni de centres commerciaux •Il n'y a pas de barrage dans les environs	Sécurité sur un site distant isolé, sans activités environnantes.	•Le site sera toujours vide en situation normale, à part quelques agents de sécurité. Ceci crée une opportunité pour des attaques	3	3	9	•Renforcer le budget pour l'infrastructure sécuritaire, car il faudra renforcer la sécurité •Consolider le système de sécurité et y inclure des systèmes de vidéosurveillance, alarmes, et détection d'intrusion physique dans les environs et à l'intérieur du site et qui fait l'objet de monitoring. •Y relier un générateur de secours et des panneaux solaires. •Prévoir des protections périphériques adéquates, murs surélevés, opaques et solides ou blindés, avec une limitation du	2	3	6

								nombre de portes •Un contrôle d'accès évolué et rigoureux, avec des rondes de vigiles et de chiens de garde à l'intérieur et à l'extérieur du site			
			Non disponibilité de liaison à haut débit pour la reprise de l'activité	•Le site est distant de la plupart des fournisseurs d'accès mis à part Togocom	3	3	9	•Disponibilité de la liaison FH de Togocom •Possibilité de créer une nouvelle liaison BLR comme backup	3	3	9
			Catastrophes naturelles	•Perturbation météorologique •Températures extrêmes •Rayonnements •Le site ne se trouve pas à proximité de la mer	2	4	8	•Vu la distance par rapport à Lomé, les sites pourront être épargnés en cas de catastrophes naturelles à Lomé. •De même, la probabilité de catastrophes naturelles simultanées dans les deux villes est quasi nulle. •Les sites étant loin de la mer, au minimum 13 Km, il n'y a pas de risque de Raz-de-marée	1	4	4
			Conflit social	•Inaccessibilité du site à cause de mouvements sociaux pouvant entrainer l'indisponibilité des voies d'accès	3	3	9	•Faible probabilité que le conflit s'étende à toute la région maritime et chaque site est desservi par au moins deux grandes voies d'accès. •Les villes à proximité de Lomé ont une faible densité, donc les soulèvements ont moins d'impact car moins de monde	2	3	6

Proposition 2	Colocalisation avec une nouvelle agence à **SANGUERA**	•Le site se trouve dans la périphérie de Lomé •Le site ne se trouve pas dans une zone inondable, ni à proximité de la mer ou d'un cours d'eau. •Il n'y a pas de forets environnantes •Ce n'est pas une zone de fortes habitations, ni de centres commerciaux •Il n'y a pas de barrage dans les environs	Sécurité du site de repli du fait de la Colocalisation avec une agence	•Le site, Colocalisé avec une agence ne sera pas vide en permanence. Cela créerait de l'activité dans la zone, diminuant ainsi les risques d'attaques mais introduisant le risque de connaissance du site backup par le grand public	3	3	9	•Séparer totalement les entrées de l'agence et du site de repli et soustraire toutes les ouvertures aux regards des clients de la banque •Contrôle d'accès automatisé (badge, PIN ou biométrique) afin de restreindre au personnel habilité, l'entrée aux étages ou compartiments destinés au site de secours. •Sécurité à renforcer par des contrôles plus rigoureux et réguliers par un personnel habilité, vu la Colocalisation avec l'agence •Le personnel doit être formé sur les réponses à tenir en cas d'alerte sécurité •Cout de maintien de toutes les infrastructures et des charges de fonctionnement à partager avec l'agence	2	3	6
			Proximité de la liaison à haut débit	•Le site est proche de la plupart des fournisseurs d'accès	2	2	4	•Le site bénéficie de la disponibilité de plusieurs fournisseurs de haut débit	2	2	4
			Catastrophes naturelles	•Raz-de-marée •Perturbation météorologique •Températures extrêmes •Rayonnements	3	5	15	•La localisation proposée est à environ 15 Km à vol d'oiseau de la Mer, ce qui limite les risques liés à la proximité de la mer comme les raz-de-marée •Elle se trouve à	2	5	10

								environ 22 Km du siège et pourrait être épargnée en cas de sinistre au siège de BATG			
			Conflit social	•Inaccessibilité du site à cause de mouvements sociaux pouvant entrainer l'indisponibilité des voies d'accès	3	4	12	• Le site proposé se trouve à au moins 22 Km du siège de la BATG et est desservi par 2 grandes voies d'accès ; cela limite la probabilité que les accès soient totalement bloqués •La zone a une faible densité, donc les soulèvements auront moins d'impact car il y a moins de monde	3	3	9

En conclusion, la proposition 1 de construction d'un nouveau site physique, comporte le moins de risques pour l'implantation d'un site de repli (25 contre 29 pour la proposition 2). Cependant, pour que celui-ci soit utilisable, nous devons définir au préalable les conditions, les procédures et dispositifs à mettre en place pour que le repli sur le site de secours se fasse dans les meilleures conditions. C'est l'objectif du chapitre qui suit.

CHAPITRE 4 : DĒFINITION DES SOLUTIONS DE SECOURS

4.1. PLAN DE REPLI ET LOGISTIQUE

Le plan de repli est le dispositif nécessaire à la reprise de l'activité en cas de sinistre déclaré affectant les locaux habituels de la banque. Il se compose :

- ➔ Du site de repli ou doivent se replier les ressources définies comme critiques pour la continuité de l'activité.
- ➔ Des procédures et de la documentation de secours pour les utilisateurs, comme les différents plans tels les plans de secours métier, informatique et télécom, etc. qui composent le plan de reprise global.
- ➔ De l'organisation de crise à déployer lors du sinistre, c'est-à-dire les personnes à mobiliser, les procédures de réunions pour le déclenchement, etc.

4.2. PLAN DE SECOURS MĒTIERS

4.2.1. Besoins pour le secours métiers

Les activités et processus critiques ont été recensés dans chaque département et l'impact de leur arrêt ainsi que la DMIA ont été évalués. La liste complète est donnée dans le tableau 13 référencé plus haut pour tous les services et départements. L'exploitation/réseaux informatique, étant la base d'une grande partie de l'activité de la banque, ne peut être interrompue que pendant maximum 24h.

Dans le cadre du secours métier, l'une des requêtes en cas de sinistre affectant le siège de la banque, était d'avoir accès à quelques agences pour effectuer les gros paiements qui ne sont pas faisables par guichet, ou pour rediriger les autres activités de caisse, de service clients et de transferts en tous genres. C'est pourquoi il est aussi nécessaire dans le plan de continuité d'activités de secourir quelques agences.

4.2.2. Secours agences

Le plateau du site de repli n'est pas propice aux activités de caisse. Les clients de la Banque ne pourront pas y être redirigés en cas de sinistre au siège et les autres agences seront déconnectées. Pour cela, 6 agences ont été sélectionnées et devront être connectées au site secours pour que les activités de caisse et de service client y soient redirigées.

Le choix proposé des agences s'est fait en tenant compte de la distance par rapport au siège pour limiter les risques que le même sinistre qui atteint le siège affecte aussi ces agences, la facilité pour les clients du siège d'y accéder, une distribution équilibrée dans la ville de Lomé ainsi que leur capacité d'accueil.

Nous avions au préalable opté pour un choix en fonction du poids financier de chaque agence, pour limiter en termes de volume les pertes liées à un sinistre affectant le siège, mais ces statistiques n'étaient pas disponibles au niveau de la Banque.

Ainsi, les agences retenues sont :

- ADIDOGOME.
- AGOE.
- GTA.
- HEDZRANAWOE.
- ECOMARINE.
- ASSIGANTO.

4.3. PLAN DE SECOURS INFORMATIQUE ET TĒLĒCOM (PSI)

Le Plan de Secours Informatique (PSI) a pour but de garantir la survie du système d'information de l'entreprise. Il permettra la continuité (en mode dégradé ou non) ou le redémarrage de l'activité le plus rapidement possible et avec un minimum de pertes de données. Il est l'un des composants essentiels d'un PCA. Il décrit ainsi la démarche à adopter pour la gestion du volet informatique et télécommunication lors de la survenance d'une situation de crise ou le PCA est déclenché. Il met en œuvre les mesures opérationnelles d'urgence pour l'accompagnement du métier.

Selon les recommandations du groupe [Cf. Référence PCA-PSI V0.1] [11], une cellule de crise Informatique doit être créée au moment de la mise en place du plan de gestion de crise qui rend compte à toutes les étapes de la crise et travaille en étroite collaboration avec la Cellule de Crise Décisionnelle (CCD). Le PSI se décline ainsi en 6 phases distinctes.

4.3.1. Description de la Cellule de Crise Informatique (CCI)

Lorsque la décision de déclencher le PCA est prise par la cellule de crise décisionnelle (CCD), sa contrepartie informatique qui est la cellule de crise Informatique (CCI), est chargée de la mise en œuvre de tous les moyens informatiques nécessaires au bon déroulement du PCA. Elle réalise le diagnostic sur le plan technique et propose des scénarios de reprise. En fonction de la nature et de l'étendue de la crise, la CCI pourra solliciter des personnes externes pour expertise dans des domaines spécifiques (Exemple : cyber-attaque).

Cependant, les hypothèses ci-dessous devront être satisfaites pour une mise en œuvre réussie du PSI :

- ➔ Le site de repli n'est pas affecté par le même événement qui perturbe le siège.
- ➔ Le stockage de données hors site et la connectivité à distance sont intacts et non affectés par le même événement qui perturbe le site primaire.
- ➔ Les procédures de sauvegarde d'informations et de restauration hors site sont existantes et opérationnelles afin de mettre en œuvre la restitution des informations critiques dans les délais de reprise d'activités arrêtés pour chaque fonction de l'entreprise.

Suivant les recommandations du Groupe, la CCI doit se composer des personnes ci-après :

- ➔ Un coordonnateur : le Responsable Informatique.
- ➔ Un membre 1 : Responsable de l'organisation.
- ➔ Un membre 2 : Représentant du Système informatique à ABI.
- ➔ Un correspondant du PCA (CPCA) : (Personne à désigner à l'IT).

4.3.2. Phases du PSI

Lorsqu'un sinistre survient, et que la décision d'activer le PCA est prise par la CCD, il est exécuté suivant les différentes phases (Cf. Référence PCA-PSI V1.0) [11] présentées sur la figure 17 :

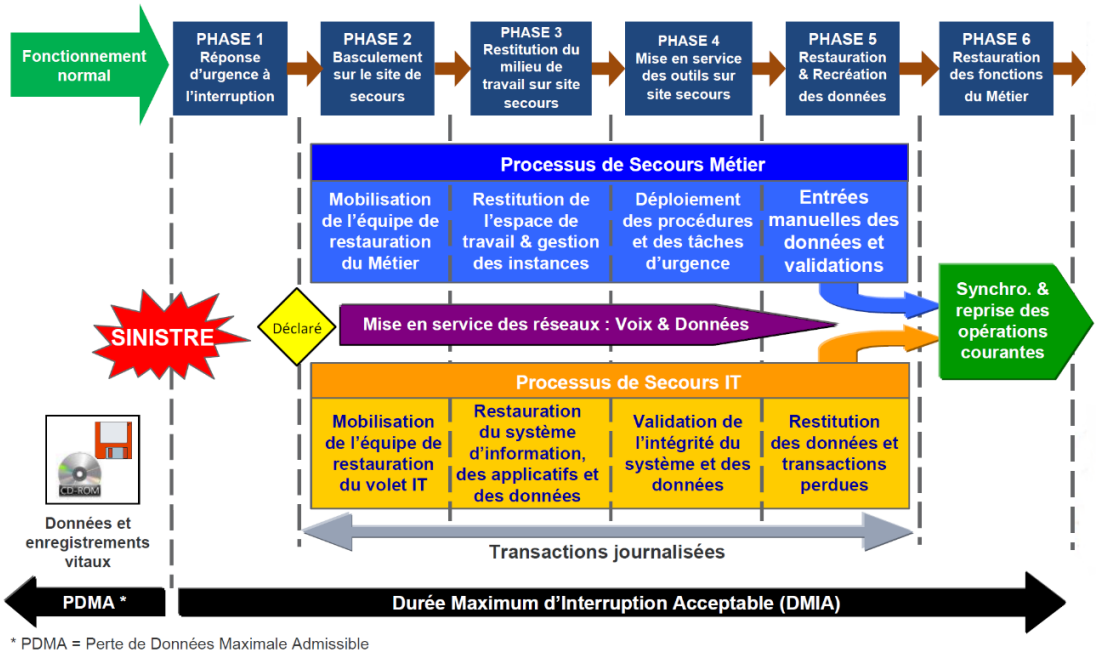


Figure 17 : Phases du PSI.

4.3.2.1. Phase 1 : Réponse d'urgence au sinistre

Le sinistre est déclaré et la CCD décide de l'activation du PCA.
La direction Risques et Contrôle a estimé la DMIA des départements Réseau Télécom et sécurité ainsi que l'Exploitation Informatique à 24h. La restauration du volet IT doit donc se faire en 24h au maximum.

4.3.2.2. Phase 2 : Mobilisation de l'équipe de restauration du volet IT

À cette étape, le sinistre est déclaré, et le PCA est effectivement activé par la CCD. Le personnel concerné par le PCA est redéployé sur le site de repli par la cellule de crise des ressources humaines et logistiques (CCRHL).

Le coordonnateur de la CCI en relation avec la CCRHL vérifie toutes les ressources humaines nécessaires au PSI afin de s'assurer de la disponibilité de chacune d'entre elles, ou alors de leur suppléant dans le cas contraire.

Le coordonnateur de la CCI est également chargé de collecter d'éventuels besoins spécifiques exprimés par les membres de sa cellule et qui n'ont pas été préalablement identifiés dans le processus et de rappeler à chaque personne le rôle qui est le sien par rapport aux tâches à accomplir dans le cadre des processus du SI retenus comme critiques.

Un compte rendu est ensuite envoyé par le coordonnateur de la CCI à la CCD sur le bouclage de cette étape et des difficultés rencontrées au fur et à mesure qu'elles surviennent.

4.3.2.3. Phase 3 : Restitution du Système d'information, des applications et des données

L'équipe de la CCI va procéder aux vérifications des prérequis en s'assurant de la disponibilité et du bon fonctionnement de tous les équipements du SI devant permettre la reprise de l'activité.

La CCI va également restaurer la configuration du SI, les données informatiques en date de la dernière sauvegarde ainsi que toutes les applications nécessaires à la bonne reprise des processus critiques.

Un compte rendu sera également envoyé par le coordonnateur de la CCI à la CCD pour l'informer du bouclage de cette étape.

4.3.2.4. Phase 4 : Mise en service des outils et validation de l'intégrité du système et des données

Au cours de cette étape, les opérations de vérification de l'intégrité des données par la CCI, suivant un canevas sont effectuées en collaboration avec la Cellule de Crise Métier (CCM) qui devra également confirmer la mise à disposition des informations d'exploitation.

Par la même occasion et en relation avec la CCM, les tests liés aux utilisateurs sont effectués afin de s'assurer qu'ils ont les bonnes habilitations pour effectuer les tâches qui leur sont confiés dans le cadre du fonctionnement sur le site de repli. En cas de nécessité, des réajustements sont apportés à la configuration du système avec le respect de la procédure et validation de la hiérarchie.

Un compte rendu sera aussi envoyé par le coordonnateur de la CCI à la CCD pour l'informer de l'arrivée au terme de cette étape.

4.3.2.5. Phase 5 : Restauration et recréation des données et transactions perdues

À ce niveau d'évolution du PCA, la CCI évaluera le niveau d'actualisation des données informatiques disponibles. En exploitant les informations de journalisation générées par le système informatique de la filiale et en collaboration avec la CCM, la CCI

travaillera à la reconstitution des données manquantes, si toutefois il y en a, dans les bases de données informatiques.

En parallèle à la reconstitution des données perdues au niveau du système informatique depuis la dernière sauvegarde, les informations déjà collectées et validées seront progressivement saisies dans la base de données.

Une fois de plus, un compte rendu sera envoyé à fréquence régulière par le coordonnateur de la CCI à la CCD sur la situation d'évolution des mises à jour ainsi que lors du bouclage de l'étape.

4.3.2.6. Phase 6 : Restauration des fonctions du métier

À cette étape, les fonctions critiques de l'entreprise sont opérationnelles de manière quasi-normale. Toutes les interdépendances commerciales et technologiques sont rétablies et la reprise des opérations commerciales de base se produit.

À cet effet, le responsable du PCA doit effectuer des validations formelles avec les coordonnateurs des différentes Cellules de Crise, qui auront pris à leur tour le soin de faire également le point avec leurs équipes respectives, afin de s'assurer que l'ensemble des opérations commerciales liées aux fonctions critiques sont prêtes pour la reprise de l'activité de la filiale.

Comme à chaque étape antérieure, un rapport sera envoyé par le coordonnateur de la CCI à la CCD, qui se chargera par la suite de diffuser les messages relatifs à la reprise effective de l'activité, ainsi que toutes les modalités pratiques y relatives.

4.3.2.7. Besoins métiers à secourir

Le responsable de chaque département a fait une liste exhaustive des effectifs, services et applications critiques à secourir en cas de sinistre majeur. Cette base détermine les exigences métier qui servent de point d'entrée pour les fonctions et applications à secourir au département Informatique.

Le tableau 16 est un résumé des applications et serveurs à secourir :

Tableau 16: Besoins Métier à secourir.

EXIGENCES METIERS	SERVEURS	APPLICATIONS	PDMA (Perte de données maximale admise)	PROCEDURE DE BACKUP	FREQUENCE
ACS	BATGSRV-ACSPROD	ACS	24H	OUI	24H
ACS	BATGSRV-ACSCOR	ACS FOR CORPORATE	24H	OUI	24H
AFRI-PAIE	BATG-SRV-PAIE	AFRI-PAIE	MENSUEL	OUI	MENSUEL
CIP	BATGSRV-CIP	CIP	N/A	NON	NON
DEPASSEMENT/CONFIRMATION	BATG-DEC	DEPASSEMENT/CONFIRMATION	24H	OUI	24H
Dossiers de partage	DCAT2 - BATG		72H	OUI	72H
EFRONT	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
ETATS COMPTABLES	DCAT2 - BATG		24H	OUI	24H
IMMOTECH	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
IMPUTATION BUDGETAIRE	SVR-BATG-SFTP	Imputation_Budget	NON	NON	NON
ORION	LOGE A ABI	Application logée à ABI	Géré par ABI	OUI	Géré par ABI
OUTLOOK	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
POWERCARD	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
PRICER	DCAT2 - BATG	Fichier	N/A	N/A	N/A
RTGS	RTGS-BATG	RTGS	24H	OUI	24H
SAGETIL	LIAISON BCEAO	Application logée à la BCEAO	Géré par la BCEAO	N/A	Géré par la BCEAO
SIRON AML	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
SIRON EMBARGO	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
SIRON KYC	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
SWIFT	LOGE A ABI	Application logée à ABI	Géré par ABI	N/A	Géré par ABI
WORC	BATG-SRV-WORC	WORC	24H	OUI	24H

Les sauvegardes se font de manière séquentielle, selon les serveurs ou les applications, comme stipulé dans le tableau 16. Certains sont journaliers, d'autres mensuels et d'autres sont gérés par ABI ou la BCEAO.
Les sauvegardes se font sur des bandes et sont conservées dans un coffre ignifuge dans les locaux même de la banque. Ils sont transférés dans un deuxième coffre ignifuge situé sur le site de repli provisoire chaque semaine.

4.3.2.8. Restauration réseaux et Télécom

Pour une continuité sans encombre, le site de repli devra être au préalable entièrement fonctionnel, c'est-à-dire les serveurs déjà sur le site et configurés, les bureaux, les desktops, les imprimantes, les scanners, les téléphones fixes, etc., déjà installés et configurés. Tous les paramétrages doivent avoir été faits, ainsi que les habilitations des utilisateurs, les user Name/password, la connectivité, etc., vérifiés.

Les données conservées sur le site de repli au moyen de bandes doivent à ce moment-là, être restaurées.

De même, les données des utilisateurs sauvegardées à la veille ainsi que les bases de données à jour-1 doivent être restituées.

Les routes doivent être mises à jour. Le trafic des agences doit être re-routé vers le site de repli.

Les 6 agences sélectionnées pour être secourues doivent toutes avoir idéalement une liaison BLR en backup, c'est-à-dire qu'il faudrait investir dans des radios à installer dans chacune des agences et une base sur le site de repli. Elles seront ainsi en permanence connectables par simple routage sur le site secours. Cette solution, bien qu'onéreuse, semble la plus appropriée ; car en temps de crise et le chaos qui y règne, la tâche de trouver un prestataire pour monter sur les pylônes et rediriger ou installer des radios peut s'avérer problématique.

4.4. GESTION DE LA CRISE

Le plan de gestion de crise intègre les moyens ainsi que l'ensemble des procédures organisationnelles et techniques permettant de se préparer et de faire face à l'apparition d'une crise. Ce plan évolue à la survenance de chaque crise, s'améliorant à partir de l'expérience de chacune des crises précédentes, ce qui permet une amélioration de la vision prospective de la gestion de crise.

Le Mémo interne No 007/19/BATG/DG/DRC du 25/09/2019 [12], décide de la mise en place d'un organe de gestion du PCA conformément à la règlementation relative à la gestion des risques dans les établissements bancaires.

Ainsi, afin d'assurer le pilotage du PCA, le mémorandum avait été tenu en vue d'une désignation formelle des membres de la cellule de gestion du plan et pour effectuer une mise à jour des différents organes de pilotage, c'est-à-dire :

- ➔ Les responsables du PCA.
- ➔ Les correspondants du PCA.
- ➔ Les membres de la cellule du PCA.

4.4.1. Le Responsable du Plan de Continuité d'Activité (RPCA)

Il s'agit de la personne en charge du déploiement du PCA, de la mise à jour et de la supervision des tests relatifs à ce plan. À ce titre, le RPCA est désigné pour coordonner les activités relatives a :

- ➔ La promotion du document de « Politique générale et gouvernance du PCA ».
- ➔ La gestion du référentiel de continuité.
- ➔ La méthodologie d'accompagnement de toutes les entités de la filiale.
- ➔ La formation et la sensibilisation du personnel.
- ➔ La gestion du système documentaire du PCA.
- ➔ La définition des plans de test du PCA.

Le directeur Risques et Contrôle de la filiale est désigné comme RPCA. Il peut également se faire assister par des expertises internes pour mener à bien sa mission.

4.4.2. Les correspondants du Plan de Continuité d'Activité (CPCA)

Les CPCA sont les principaux collaborateurs du RPCA. Leur rôle principal est d'assister le RPCA dans l'accomplissement de ses missions.

Ils sont formellement identifiés au niveau des différentes fonctions de l'établissement : FINANCES et COMPTABILITE, RESSOURCES HUMAINES, TRESORERIE, COMMUNICATIONS, LOGISTIQUES et IMMOBILISATION, OPERATIONS, RISQUE et CONTRÔLE, BANQUE DE L'ENTREPRISE, ENGAGEMENTS, BANQUE DE DETAIL, JURIDIQUE et GOUVERNANCE, ORGANISATION et QUALITE, IT.

Ce sont les personnes ressource en charge de véhiculer l'information sur les anomalies ou incidents pouvant occasionner un arrêt ou induire une désorganisation ou

une compromission de la continuité des activités. Ils doivent s'assurer de remonter toutes les informations relatives au RPCA ou à la Cellule de Remontée des Incidents Majeurs (CRIM).

4.4.3. Définition des cellules de crise

La cellule de crise constitue la « tour de contrôle » de tous les évènements qui se déroulent pendant la crise, depuis le déclenchement jusqu'à la résolution complète. Ce sont les organes essentiels à la gestion de la crise. Ces cellules sont dotées d'un ensemble de modes d'organisation et de techniques qui permettent de se préparer à faire face à la survenance d'une crise, puis d'en tirer les enseignements afin d'améliorer son organisation.

Les différentes cellules doivent être constituées pour assurer de manière proactive les activités de gestion de crises.

À cet effet, à la suite du Mémo interne [12], 6 cellules ont été définies dans le cadre de la gestion du PCA.

4.4.3.1. La Cellule de Crise Décisionnelle (CCD)

La CCD est l'organe principal de coordination de l'ensemble des activités suite à la déclaration d'un sinistre, et ce, jusqu'à sa résolution complète.

Dans le cadre de note étude, la CCD nous concerne dans son rôle de décision de l'activation ou non du PCA, ainsi que la coordination jusqu'au déplacement sur le site de repli. La résolution complète de la crise et la reprise de l'activité ne font pas partie du cadre de notre étude.

Les membres de la CCD sont définis dans la figure 18 :

N°	Fonction	Statut
1	Directeur Général	Coordonnateur
2	Directeur Risques & Contrôle	Responsable du PCA
3	Directeur Général Adjoint	Membre
4	Directeur Audit Interne	Membre
5	Directeur Banque de Détail	Membre
6	Directeur Banque de l'Entreprise	Membre
7	Directeur Juridique et Gouvernance	Membre
8	Directeur des Engagements	Membre
9	Directeur des Opérations	Membre
10	Directeur des Ressources Humaines	Membre
11	Directeur Financier & Comptable	Membre
12	Directeur de la Trésorerie	Membre
13	Responsable Organisation & Qualité	Membre
14	Chef Service Logistique et Immobilisations	Membre
15	Responsable Communication	Membre
16	Responsable Informatique	Membre

Figure 18 : Membres de la CCD.

Le directeur Général est le coordinateur de la cellule de crise décisionnelle. En cas de sinistre, il réunit formellement les membres de la CCD et décide sur l'activation du PCA. Il répartit ainsi les actions à déployer pour gérer efficacement la crise.

4.4.3.2. La cellule des Remontées des Incidents Majeurs (CRIM)

La CRIM est chargée de la remontée en temps réel au RPCA, des incidents pouvant avoir un impact négatif sur la continuité d'activité.

La cellule est composée de personnes identifiées dans les principales directions et dont la mission est d'alerter en cas de survenance d'incidents dans leurs directions.

Les membres de la CRIM sont définis dans la figure 19 :

N°	Fonction	Statut
1	Directeur Risques et Contrôle	Coordonnateur
2	Chef Service Contrôle des Opérations	Membre
3	Chef Service Surveillance des Engagements	Membre
4	Chef Service Sales (Trésorerie)	Membre
5	Chef Service Logistique et Immobilisations	Membre
6	Chef Service Administration et Paie	Membre
7	Responsable Organisation & Qualité	Membre
8	Responsable Informatique	Membre

Figure 19 : Membres de la CRIM.

Le directeur Risques et Contrôles est le Coordinateur de la cellule des Remontées des incidents Majeurs.

4.4.3.3. La Cellule de Crise Métier (CCM)

La CCM est chargée de l'exécution opérationnelle du PCA en collaboration avec le CCD. Elle identifie les personnes clés métiers pour la gestion de la situation de crise. La cellule définit les activités opérationnelles pour gérer la crise.

Elle se compose comme suit dans la figure 20 :

N°	Fonction	Statut
1	Directeur Risques & Contrôle	Coordonnateur
2	Directeur Général Adjoint	Membre
3	Directeur Banque de Détail	Membre
4	Directeur des Engagements	Membre
5	Directeur des Opérations	Membre
6	Directeur Financier & Comptable	Membre
7	Directeur de la Trésorerie	Membre
8	Responsable Organisation & Qualité	Membre
9	Chef Service Back-Office Monétique	Membre

Figure 20 : Membres de CCM.

Le directeur Risques et Contrôles est le Coordinateur de la cellule de Crise Métiers.

4.4.3.4. La Cellule de Crise Informatique (CCI)

La CCI est chargée de la mise à disposition de tous les moyens informatiques nécessaires au bon déroulement du PCA en collaboration avec la CCD.
Selon la nature et l'étendue de la crise, la CCI pourra solliciter des expertises internes ou externes dans certains domaines comme l'énergie, les études, les Télécom, etc.

Les membres de la CCI sont définis dans la figure 21 :

N°	Fonction	Statut
1	Responsable Informatique	Coordonnateur
2	Directeur Risques & Contrôle	Responsable du PCA
3	Responsable Organisation & Qualité	Membre
4	Représentant Pôle Organisation et Système d'Information - ABI	Membre
5	Informaticien	Correspondant du PCA

Figure 21 : Membres de la CCI.

Le responsable informatique est le Coordinateur de la CCI

4.4.3.5. La Cellule de Crise Ressources Humaines et Logistiques (CCRHL)

La CCRHL est chargée de la coordination du PCA sur le périmètre des Ressources Humaine, notamment dans la désignation des personnes ressources pour la conduite des activités à maintenir ; ceci en collaboration avec la CCM et la CCD.

En fonction de l'étendue de la crise, la cellule pourra solliciter des expertises internes ou externes dans des domaines de compétences spécifiques comme les assurances, la sécurité des biens et des personnes, le courrier, le transport, la logistique, le courrier, etc.

Les membres de la CCRHL sont les définis dans la figure 22 :

N°	Fonction	Statut
1	Directeur des Ressources Humaines	Coordonnateur
2	Directeur Risques & Contrôle	Responsable du PCA
3	Directeur Financier & Comptable	Membre
4	Chef Service Logistique et Immobilisations	Membre
5	Chargé de la Logistique	Correspondant du PCA

Figure 22 : Membres de la CCRHL.

Le responsable des Ressources humaines est le coordinateur de la cellule de crise des RH et logistiques (CCRHL)

4.4.3.6. La Cellule de Communication de Crise (CCC)

La CCC est chargée de préparer un plan de communication de crise en collaboration avec la CCD, la CCM, la CCI et la CCRHL.

Elle est la seule habilitée à gérer transversalement les communications lors de la survenance de crise majeure. Elle constitue l'organe essentiel pour la bonne gestion de la crise par la Direction Générale notamment dans la communication avec les parties prenantes (Client, régulateur, CAC, partenaires).

La cellule de Communication de Crise est composée des membres ci-après dans la figure 23 :

N°	Fonction	Statut
1	Responsable Communication	Coordonnateur
2	Directeur Risques & Contrôle	Responsable du PCA
3	Directeur General Adjoint	Membre
4	Directeur Ressources Humaines	Membre
5	Directeur Juridique et Gouvernance	Membre
6	Chef Service Logistique & Immobilisations	Membre

Figure 23 : Membres de la CCC.

Le responsable Communications est le coordinateur de la Cellule de Communication de Crise.

Les listes de contacts

En temps normal, il est déjà souvent difficile de joindre quelqu'un ; que dire alors en cas de sinistre ! La liste des contacts a donc pour fonction d'établir précisément le rôle de chaque employé, en donnant ses coordonnées ainsi que la personne le remplaçant en cas d'absence ou d'indisponibilité.

C'est un véritable outil entre les mains des responsables du plan de continuité. Ces listes doivent être établies avec le plus grand soin, dans le respect des contraintes dues à leur usage.

Chaque entité potentiellement impliquée dans des actions de réaction face à un sinistre (départements en support opérationnel, départements métier) doit tenir à jour une liste des employés qui seront sollicités pour mener à bien ces actions. Ces listes doivent être faciles à trouver, lisibles et mises à jour régulièrement (Un annuaire PCA).

La DRC a établi la liste des personnes critiques pour les activités à maintenir ainsi que leur back up. Les informations relatives à l'adresse mail et aux numéros de téléphone doivent être jointes pour compléter l'annuaire. La liste est dans le tableau 17 :

Tableau 17 : Personnes critiques et leur backup.

FONCTIONS		**CONTACT**		
PERSONNES CRITIQUES	**BACKUP DES PERSONNES CRITIQUES**	**NOM**	**MAIL**	**Numéros de téléphone**
Chef de Caisse	Caissier Principal			
Directeur des Opérations	Directeur Adjoint des Opérations			
Chef Service Portefeuille Local	Chef Service Étranger			
Agent chargé des opérations bancaires	Autre agent chargé des opérations bancaires			
Chef Service Étranger	Directeur Adjoint des Opérations			

Chef Service Étranger	Chef Service Portefeuille Local			
Chargé des Transferts Internationaux	Chargé de la réglementation de change			
Chef Service Back-Office Monétique	Chef Service Étranger			
Agent chargé des opérations bancaires	Chargé des DABs			
Responsable Informatique	Exploitant Informatique			
Directeur de la Trésorerie	Chef Service Sales			
Responsable Organisation et Qualité	Assistant Organisation et Qualité			
Directeur des Engagements	Chargé de la Contre-Étude			
Directeur Général	Directeur Juridique et Gouvernance			
Directeur des Engagements	Chef Service Surveillance des Engagements			
Directeur Banque de l'Entreprise	Chef Service Institutionnels			
Chef Zone, Intérim Directeur Banque de Détail	Chef Service Crédit aux Particuliers et Professions Libérales			
Chef Service Administration des Engagements	Administrateur des Engagements			
Chargé de la compensation	Agent des opérations			
Directeur Juridique et Gouvernance	Assistant Juridique			
Chef Service Surveillance des Engagements	Administrateur des Engagements			
Chef Service Logistique et Immobilisations	Chargée de la Logistique			
Chargé de la Sécurité	Chargé de la Logistique			
Comptable chargé des reportings	Directeur Financier et Comptable			
Chef Service Contrôle Comptable	Contrôleur Comptable			
Chef Service Cash Management & Trade	Chargé d'Affaires Trade			
Chef Service Administration et Paie	Chef Service GPEC			

4.4.3.7. Maintien en condition opérationnelle du PCA

L'objectif premier du maintien en condition opérationnelle est d'identifier les points clés des contrôles à effectuer pour s'assurer que le PCA est opérationnel et le reste dans la durée.

Le plan doit être vivant et faire l'objet de contrôles réguliers :

- ➔ Vérifications périodiques.
- ➔ Entretien des dispositifs de secours.
- ➔ Tests des procédures de bascule.
- ➔ Exercices et entraînement (simulés ou réels).
- ➔ Tenue à jour du plan.
- ➔ Mesure du niveau de maturité.
- ➔ Révision des procédures et dispositifs.
- ➔ Documenter les retours d'expérience.

Il est recommandé qu'une copie (papier et/ou numérique) de la documentation soit stockée sur un site distant, dans un lieu sécurisé et accessible (le site de repli par exemple).

Les exercices sont un moyen pertinent pour valider l'efficacité du PCA. Chaque exercice doit être pensé et organisé en fonction de ce que l'on veut vérifier. Il peut s'agir par exemple de vérifier :

- ➔ La procédure d'alerte.
- ➔ Le fonctionnement de la cellule de crise (par un exercice simulé, avec activation de la cellule de crise).
- ➔ Les procédures techniques de basculement en mode secours (par la mise en œuvre réelle et périodique).
- ➔ La coordination des différentes parties prenantes, lors d'un exercice de réponse à un incident grave simulé par exemple.

Il est préconisé de s'assurer que la formation du personnel aux procédures techniques a bien été ciblée et réalisée avant de déclencher les premiers exercices. Les éléments critiques du PCA doivent impérativement être testés au moins une fois par an !

4.5. PROCESSUS PCA : LOGIGRAMME

Pour résumer le processus d'enclenchement du PCA ainsi que les étapes à suivre jusqu'au déplacement sur le site de repli et la reprise de l'activité, un logigramme spécifiant qui, quoi et comment, est fourni dans la figure 24 :

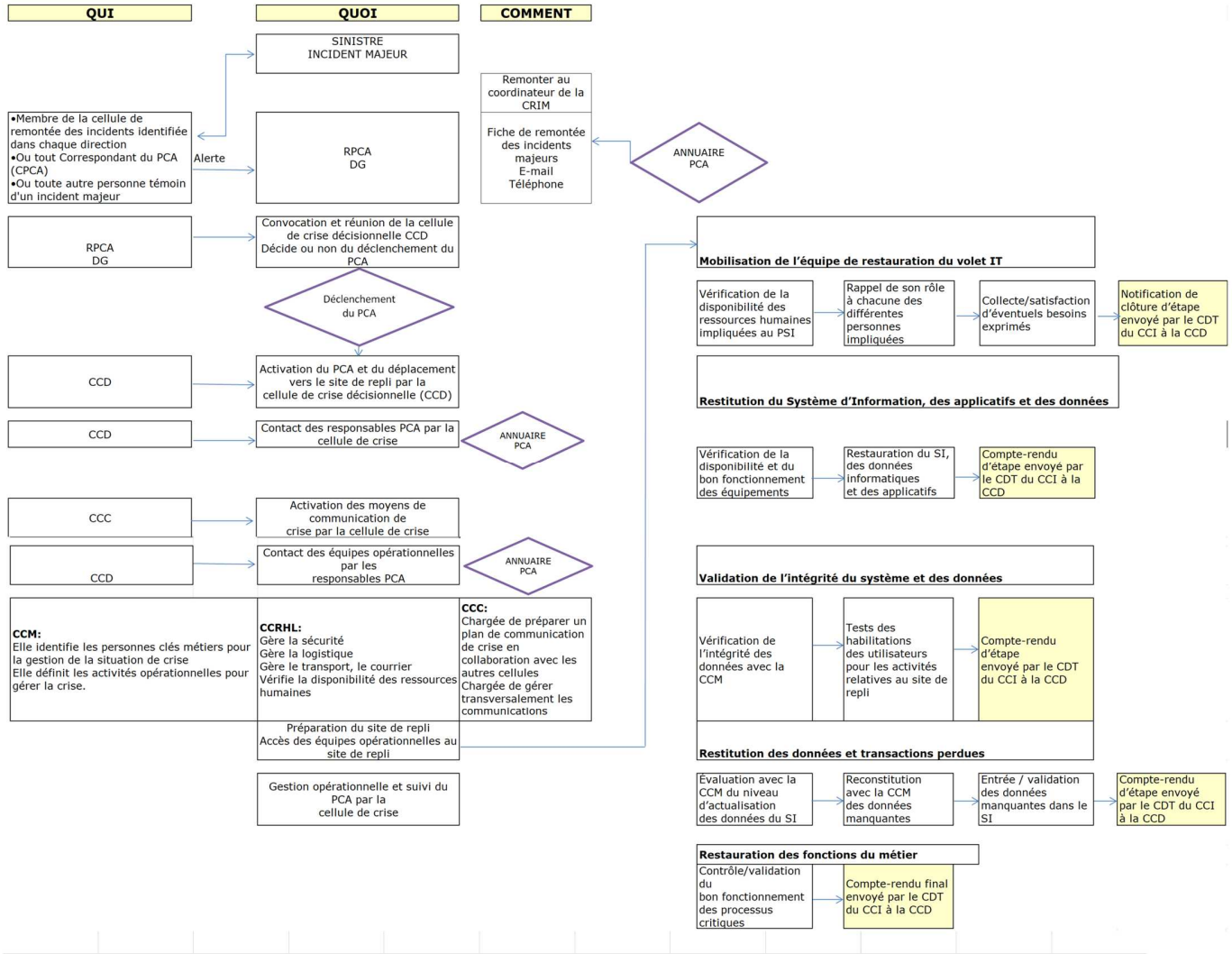


Figure 24 : Logigramme processus PCA.

CHAPITRE 5 : ĒVALUATION DU COUT DU PROJET

5.1. SITUATION GĒOGRAPHIQUE DU SITE RETENU

Le site que nous avons retenu pour l'évaluation du coût du projet est le site dans la ville de NOEPE qui est la troisième option proposée. La ville se trouve à environ 28 km du siège. Les sites dans ces différentes localités ont le même ordre de grandeur de coûts.

Notre choix s'est porté sur cette localité en raison de son accessibilité par rapport aux autres localités proposées. Elle se trouve à l'intersection de quatre grandes voies distinctes, l'une non bitumée qui passe par Kovié ; les trois autres bitumées dont le Boulevard du 30 Août, une extension de la Nationale 1, et l'autre passant par le Ghana (39 Km). Ceci représente une porte de sortie avantageuse en cas de problème ou soulèvement majeur dans la ville de Lomé (Figures 25, 26, 27 et 28).

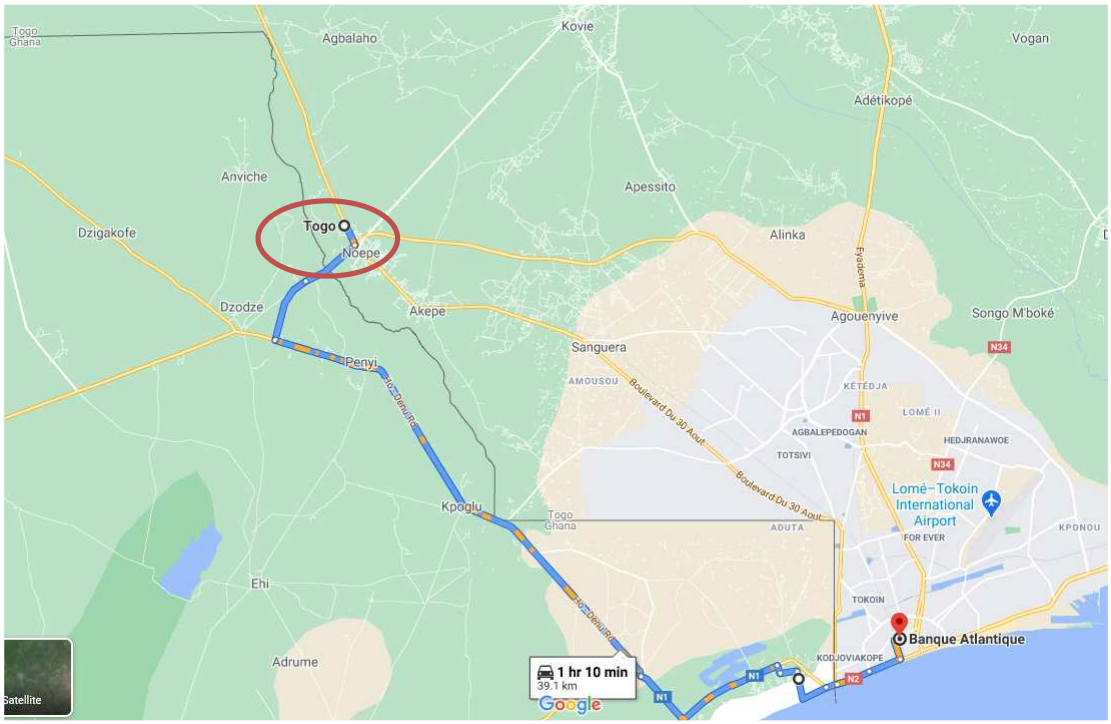


Figure 25 : Position site de repli de NOEPE.

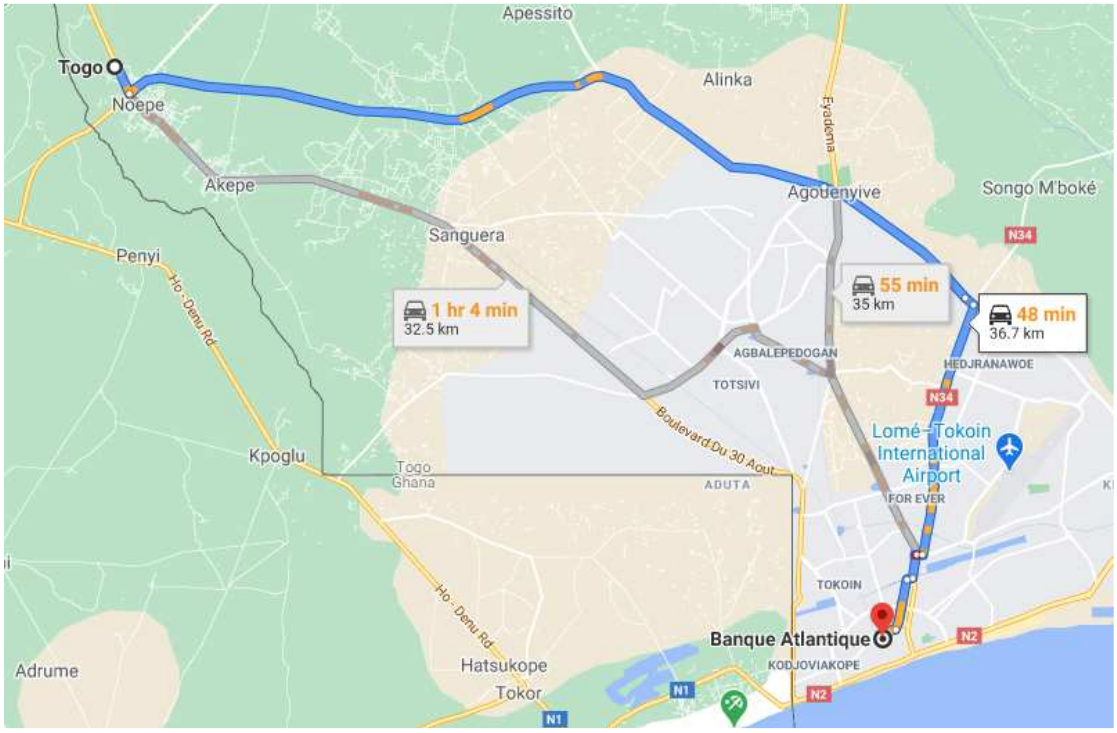


Figure 26 : Site de NOEPE, routes.

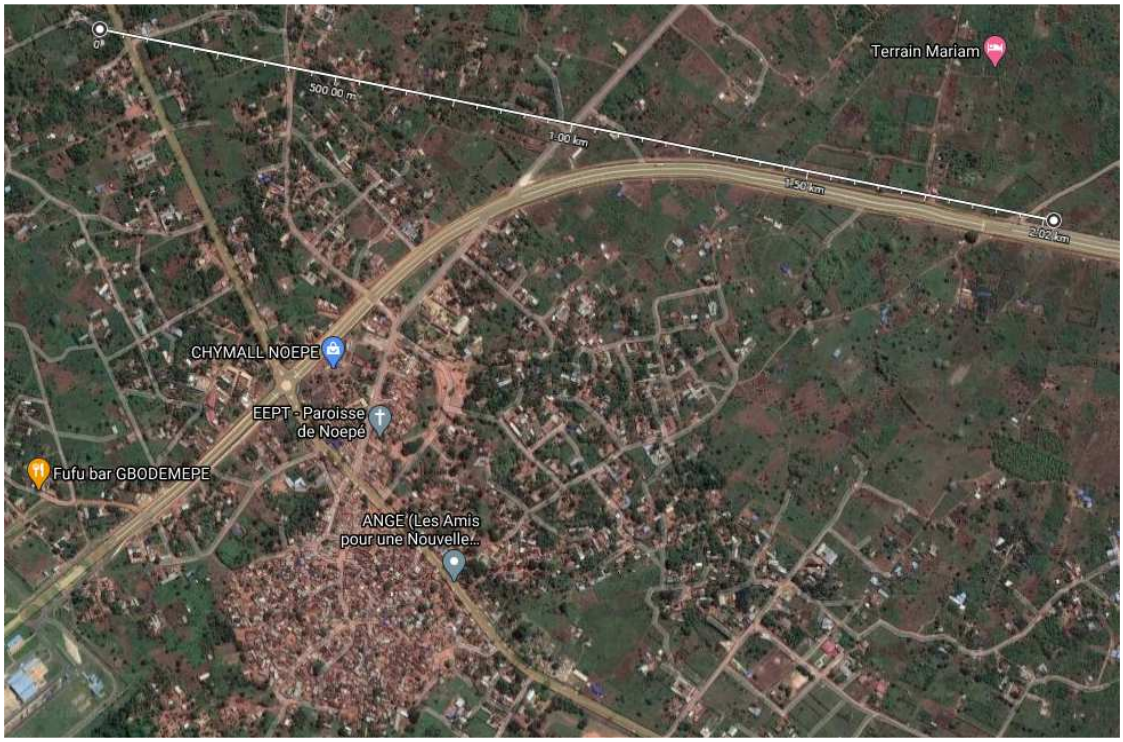


Figure 27 : Site de NOEPE, Satellite.

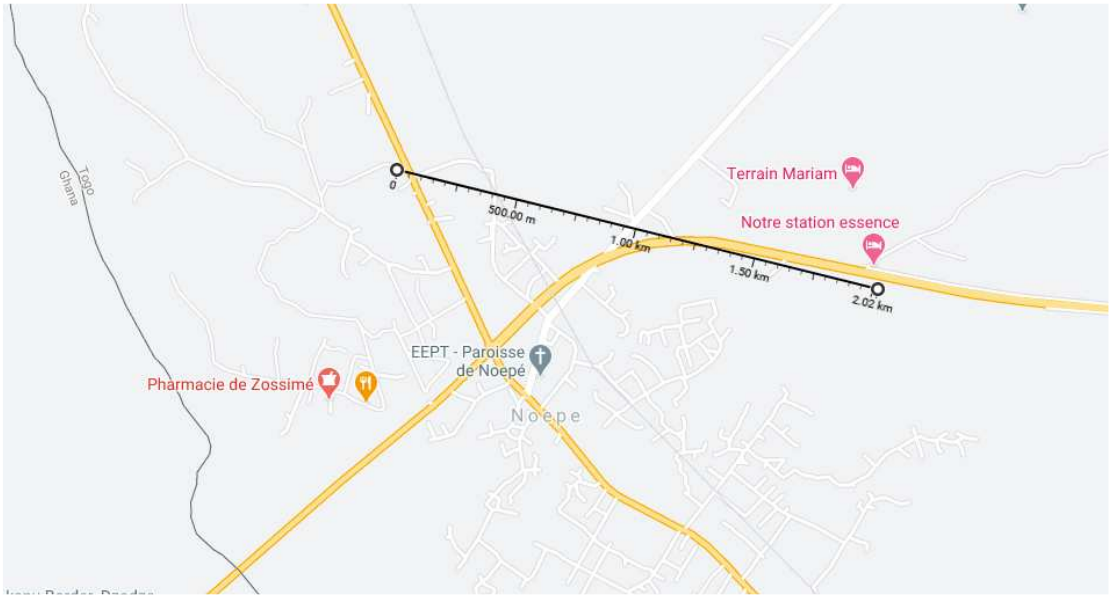


Figure 28 : Site de NOEPE Coordonnées.

Les coordonnées du site de Noepe sont : (6.269537368718644, 1.0316124485226095).

5.2. ÊVALUATION DU COUT DES INFRASTRUCTURES

D'après les évaluations, le site devra avoir une superficie d'au moins 142.8 m². Il va donc s'agir d'évaluer le coût d'un bâtiment d'environ 150 m² de surface habitable auquel il faudra ajouter toutes les exigences techniques et sécuritaires décrites en [3.4.1]. Le coût des équipements doit y être inclus ainsi que celui de la location de la liaison FH de Togocom et/ou une nouvelle liaison BLR.

5.2.1. Construction de l'immeuble

Un prestataire externe a estimé les coûts de la construction d'une nouvelle agence d'une superficie de 300 m² à Lomé, du gros œuvre, des sanitaires, des carreaux, de toutes les portes et fenêtres en aluminium, des baies vitrées blindées, de l'électricité et de la vidéosurveillance des extérieurs.

Cependant, nous n'avons besoin que d'environ 150 m² de surface construite pour le site de secours. Nous faisons ainsi une extrapolation basée sur le coût total de cette agence. À cela nous ajoutons le prix du terrain et de l'installation d'un paratonnerre. Dans le tableau 18, nous avons la proposition faite à la banque pour la construction de la nouvelle agence :

Tableau 18 : Proposition de construction d'une nouvelle agence.

NOUVELLE AGENCE (300 m²)	MONTANT (FCFA)
GROS ŒUVRE	149,974,820
ALU	42,697,427
ELECTRICITE	54,723,680
SECURITE	10,608,813
PRIX DE LA CONSTRUCTUTION DE LA NOUVELLE AGENCE	**258,004,740**

L'estimation des coûts de construction du bâtiment pour le site de secours nous donne ainsi un ordre de prix résumé dans le tableau 19 ci-dessous :

Tableau 19 : Estimation du cout de la construction du site secours.

SITE DE SECOURS (150 m²)	MONTANT (FCFA)
ACQUISITION TERRAIN (2 lots = 1200 m²)	40,000,000
GROS ŒUVRE	74,987,410
ALU	21,348,714
ELECTRICITE	40,000,000
SECURITE	5,304,407
PARATONNERRE	10,000,000
CLOTURE DE SECURITE DU TERRAIN	4,800,000
ENSEMBLE DU SITE - TOTAL 1 :	196,440,531

L'acquisition de 2 lots, c'est-à-dire 1200 m², est proposée pour une question de sécurité. Ceci limitera en effet les risques liés aux habitations voisines trop proches du site de secours, les vis-à-vis, etc. La sécurité périmétrique indispensable qui va de pair avec un site aussi isolé pourra y être appliquée.

La banque pourra aussi y délocaliser ses magasins, ses archives, etc. et diminuer ainsi ses coûts en location disparate dans la ville de Lomé.

Cependant, le bâtiment fini ne représente qu'une portion du site de secours. Il est nécessaire de l'équiper selon les exigences et standards de sécurité internationaux.

5.2.2. Équipements

Pour respecter les règles de sécurité conformes aux normes et standards internationaux, le site de secours doit être équipé de toutes les infrastructures sécuritaires recommandées par ABI ; c'est-à-dire, être doté de Vidéo surveillance, alarmes incendie, alarmes intrusion, extinction automatique de feux, aération, étanchéité, portes coupe-feu, etc. Le système de contrôle d'accès doit aussi être restreint et automatisé par des badges, des PIN ou biométrique.

Un devis quantitatif a été fait par un prestataire de service externe pour équiper la salle technique du site de secours existant de toutes ses infrastructures sécuritaires ainsi que sa sécurité électronique. Ce devis peut être applicable au site de secours dans le cadre de notre PCA. Il est donné dans le tableau 20 :

Tableau 20: Devis estimatif de la sécurité de la salle technique du site de secours et des liaisons filaires.

SALLE TECHNIQUE : SECURITE ELECTRONIQUE	ESTIMATION (FCFA)
VIDÉO SURVEILLANCE	25,000,000
SYSTÈME DE CONTRÔLE D'ACCÈS	
DÉTECTION INCENDIE ET EXTINCTION AUTOMATIQUE	
PORTE SALLE MACHINE/SALLE PUISSANCE	
SALLE SERVEUR	
FILERIE, ACCESSOIRES ET PRESTATIONS	
SYSTÈME D'INTRUSION	
CONTRÔLE ENVIRONNEMENTAL DE LA SALLE IT	
MISE EN SERVICE	
PARTICIPATION FRAIS D'INSTALLATION DES NOUVELLES LIASONS FILAIRES DE TOGOGOM POUR LES 6 AGENCES + LE SITE DE SECOURS	8,000,000
TOTAL 2 :	33,000,000

➔ Le groupe électrogène, les équipements réseau et télécom dont la VSAT ainsi que les serveurs du site de secours existant seront redéployés sur le nouveau site.

- ➔ Les 6 agences à secourir dans le cadre du PCA seront connectées avec le site de secours par la fibre de Togocom.
- ➔ La location de 7 liaisons filaires avec Togocom ainsi que la participation aux frais des installations doivent être prévues.
- ➔ Selon l'étude des besoins en effectifs du site de repli en [3.2.2.] ; 13 Ordinateurs fixes, 13 tables de bureau/fauteuils de bureau, 2 imprimantes, 1 téléphone fixe, 1 scanner et 3 cachets devront être achetés, installés, configurés et déployés d'avance sur le site de secours. L'effectif déjà présent sur le site de secours existant peut être redéployé sur le nouveau site.
- ➔ 25 personnes seront en télétravail, mais avec leurs propres ordinateurs portables déjà fournis par la banque pour leurs taches habituelles. Ils devront s'assurer de les avoir en permanence durant leurs déplacements hors du siège de la BATG, afin ne pas risquer que le même sinistre qui atteint le siège n'affecte les ordinateurs par la même occasion.

5.2.3. Coût total

En conclusion, notre site de secours est un bâtiment d'une superficie d'environ 150 m² réunissant toutes les exigences techniques et sécuritaires des normes internationales ; entièrement équipé pour accueillir l'effectif nécessaire à la continuité de l'activité de la BATG en cas de sinistre affectant le siège de la filiale. Son coût total est résumé dans le tableau 21 :

Tableau 21 : Coût final du site de secours.

TOTAL 1	196,440,531
TOTAL 2	33,000,000
COUT TOTAL	229,440,531
MAJORATION DE 10% POUR LES IMPREVUS :	22,944,053
COUT TOTAL FINAL	**252,384,584**

Le coût au final du site de secours, estimé avec une grande marge, se situe autour de 252 millions de francs CFA.

CONCLUSION GĒNĒRALE

Mettre en place un plan de continuité d'activité est un énorme projet transverse et complexe qui nécessite l'intervention de nombreuses parties prenantes, vu le caractère intégral du projet et les enjeux. Pour cela, l'implication de la Direction Générale est nécessaire pour sa réussite.

Vu la taille et la criticité de son infrastructure grandissante ces dernières années, c'est une démarche logique de s'assurer que sa continuité d'activité sera effective dans le cas où un sinistre important surviendrait, aussi bien pour ses clients, son business et son image de marque. C'est pourquoi la BATG a initié depuis 2016, le projet de mise en place d'un site de secours pour assurer la continuité de son activité. Il est à environ à 84% d'achèvement. Cependant, étant donné que le site de secours existant est toujours dans un état provisoire faute d'espace adéquat, il nous a été confié lors de notre stage à la banque, le projet de déterminer un nouveau site de repli définitif répondant aux exigences et standards internationaux. Dans cette lancée, nous nous sommes aussi attelés à l'élaboration d'un Plan de continuité d'activité globale pour la BATG.

L'élaboration d'un PCA est assez compliquée du fait qu'il est transverse et réclame la participation d'un grand nombre d'acteurs et de facteurs qu'il est important de prendre en compte pour éviter tout blocage lors de la mise en œuvre du plan.

Il nous a fallu entre autres, identifier les activités et processus essentiels à la continuité de l'activité de la Banque en cas de sinistre grave et les évaluer, puis leur attribuer des poids et les classer par criticité. Cette partie a été celle de tous les défis dans la mesure où il nous a fallu trouver des éléments de classement pertinents pour pallier l'absence de statistiques financières par département. Seules les statistiques globales étaient disponibles.

L'étape suivante était l'analyse et la cartographie des risques ainsi que l'identification de différents scénarios de crise. Vinrent par la suite les descriptions des différents plans qui composaient le plan de repli global, c'est-à-dire les plans de secours Métier, Informatique et télécom, Logistique et de Gestion de Crise.

Le PCA est un plan dynamique, vivant et en constante évolution. Il doit régulièrement être revu, testé et mis à jour afin de s'assurer de la capacité et de la possibilité de sa mise en œuvre au cas où un sinistre surviendrait. Les points clés pour la réussite de sa mise en œuvre sont la communication, la formation et l'information. Les acteurs du PCA doivent être convenablement formés et avoir une idée claire de leur rôle et des actions attendues d'eux. Les retours d'expérience doivent être soigneusement pris en compte pour permettre au plan d'évoluer.

La suite logique du travail fait dans le cadre de ce mémoire pourrait être la rédaction détaillée de la documentation et des procédures proprement dites du Plan de Continuité d'Activité global de la BATG.

RĒFĒRENCES

[1] hfds-guide-pca-plan-continuite-activite-_sgdsn
http://www.sgdsn.gouv.fr/uploads/2016/10/guide-pca-sgdsn-110613-normal.pdf

[2] Règlement 97 02 du Comité de la Réglementation Bancaire et Financière CRBF
https://www.scribd.com/document/255236860/Reglement-97-02

[3] Circulaires de la BCEAO
https://www.bceao.int/fr/documents/circulaires

[4] Norme ISO 22301
https://www.iso.org/obp/ui#iso:std:iso:22301:ed-2:v1:fr

[5] Accords Bale II
https://fr.m.wikipedia.org/wiki/B%C3%A2le_II

[6] Concevoir un Plan de Continuité d'Activités pour les applications critiques et/ou un Plan de reprise d'activité (PRA) structuré permettant de répondre à un maximum de scenarios d'incidents. Thomas Tellier. HAL archives-ouvertes.fr
https://dumas.ccsd.cnrs.fr/dumas-01681360

[7] Evaluation des risques
https://fr.wikipedia.org/wiki/%C3%89valuation_des_risques

[8] Norme ISO 31000 :2018 Management du risque
https://www.iso.org/obp/ui/fr/#iso:std:iso:31000:ed-2:v1:fr

[9] Méthode EBIOS
https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

[10] Office Space Planning Standards
https://www.inf.gov.nt.ca/sites/inf/files/office_space_standards_and_guidelines.pdf

[11] Plan de Secours Informatique (PSI) Filiale Groupe Banque Atlantique.
Référence : PCA-PSI V1.0

[12] Memo Interne_Organes de Gestion du PCA
No 007/19/BATG/DG/DRC du 25/09/2019