



**HAL**  
open science

# De l'étude de risque à la conception de l'infrastructure optimisée dans le cadre d'un plan de continuité et de reprise d'activité informatique

Francis Yelouassi

## ► To cite this version:

Francis Yelouassi. De l'étude de risque à la conception de l'infrastructure optimisée dans le cadre d'un plan de continuité et de reprise d'activité informatique. Ingénierie, finance et science [cs.CE]. 2013. dumas-01324580

**HAL Id: dumas-01324580**

**<https://dumas.ccsd.cnrs.fr/dumas-01324580>**

Submitted on 1 Jun 2016

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE D'ENSEIGNEMENT DU BENIN

---

MEMOIRE

Présenté par **Francis YELOUASSI**

en vue d'obtenir

LE DIPLÔME D'INGENIEUR CNAM

SPECIALITE: INFORMATIQUE, SYSTEME D'INFORMATION

---

De l'étude de risque à la conception de l'infrastructure  
optimisée dans le cadre d'un plan de continuité et de  
reprise d'activité informatique

Soutenu le 18 octobre 2013

---

JURY

PRESIDENT:

Madame Isabelle WATTIAU

MEMBRES:

Monsieur Jacky AKOKA

Monsieur Thierry JAQUES

Madame Elena KORNYSHOVA

---



CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE D'ENSEIGNEMENT DU BENIN

---

MEMOIRE

présenté par **Francis YELOUASSI**

en vue d'obtenir

LE DIPLÔME D'INGENIEUR CNAM

SPECIALITE: INFORMATIQUE, SYSTEME D'INFORMATION

---

De l'étude de risque à la conception de l'infrastructure  
optimisée dans le cadre d'un plan de continuité et de  
reprise d'activité informatique

Soutenu le 18 octobre 2013

---

Les travaux relatifs à ce mémoire ont été effectués au sein de la société Oryx Bénin  
SA, sous la direction de *Messieurs Daniel Nunez et Thierry Jaques.*

---

## MEMOIRE D'INGENIEUR C.N.A.M. en INFORMATIQUE

De l'étude de risque à la conception de l'infrastructure optimisée dans le cadre d'un plan de continuité et de reprise d'activité informatique

Francis YELOUASSI

Cotonou le 18 octobre 2013

---

### Résumé

La multinationale AOG (Addax and Oryx Group), Leader dans le domaine pétrolier et minier, a impulsé un projet de mise en œuvre de plan de continuité dans toutes ses filiales. C'est dans cette dynamique, que le projet DRP (Disaster Recovery plan) a été initié au sein de la filiale du Bénin (Oryx Bénin SA) afin d'assurer la continuité et le cas échéant, la reprise rapide des activités de l'entreprise en cas de sinistre.

Ce mémoire traite de la manière dont le projet DRP a été mené. De la note de cadrage, à la conception de l'infrastructure optimisée, en passant par l'analyse d'impact sur l'activité et l'étude de risque, toutes les étapes du projet sont décrites, afin de permettre au lecteur de mieux comprendre, les enjeux et les conclusions de ma mission

**Mots-clés :** Continuité d'activité, Etude de risque, Etude d'impact, Virtualisation, Réplication

---

### Summary

Multinational AOG (Addax and Oryx Group), an industry leader in oil and mining, has spearheaded a project to implement a business continuity plan in all its subsidiaries. It is in this dynamic that the proposed DRP (Disaster Recovery Plan) was initiated within the subsidiary of Benin (Benin Oryx SA) to ensure continuity and appropriate, early resumption of activities of the business disaster.

This thesis deals with how the DRP project was conducted. The concept note, the design of optimized infrastructure, through the analysis of business impact and risk study, all stages of the project are described to enable the reader to better understand the issues and conclusions of my mission

**Keywords:** Business Continuity, Risk Study, Impact Assessment, Virtualization, Replication

---

## **Remerciements**

Ce mémoire est l'aboutissement de plusieurs années d'études au CNAM; années durant lesquels le soutien indéfectible de nombreuses personnes m'a été extrêmement utile. Je tiens à les remercier.

En premier lieu, Monsieur le professeur Jacky AKOKA qui a accepté de diriger ce mémoire. Je souhaite remercier également, Messieurs Daniel NUNEZ et Thierry JAQUES qui sont mes tuteurs en entreprise et n'ont ménagé aucun effort pour m'accompagner dans l'atteinte de cet objectif.

Ce mémoire est aussi la concrétisation d'une expérience professionnelle enrichissante au sein de la Société Oryx Bénin et je remercie Messieurs Didier VERON, Jérôme BESEME, Dominique LALES, Simon PEMONT et Florent FERNANDEZ qui ont crus en mes capacités et toute l'équipe informatique du groupe AOG, notamment mon collaborateur Alidou CHABI GANI.

Ce mémoire est surtout, une ambition personnelle qui n'implique pas que ma personne. Je pense notamment à ma mère Agnès D'ASILVA, Mes frères Roméo, Aimé, Jaques et ma sœur Marie Laurence.

Mes remerciements vont particulièrement à l'endroit de mon épouse Vinciane HOUNGBO, avec laquelle j'ai construit ce projet. A nos deux garçons Paterne et Karel et notre fille Marielle, qui je le souhaite comprennent à travers ce travail qu'au bout de l'effort, il y a toujours le réconfort.

Une pensée particulière à mon père et Ami Etienne YELOUASSI qui m'indiqua, il y de cela huit (08) ans le chemin du CNAM et qui depuis lors, n'a jamais cessé de m'exhorter à la persévérance.

A toute la promotion 2005 du Centre d'enseignement du CNAM à Cotonou, dont je suis le premier Ingénieur CNAM.

Enfin, Un grand Merci à Monsieur Claude FILLIATRE, ancien chargé de mission du CNAM pour le Bénin à qui je dédie ce mémoire.

---

## Liste des abréviations

AFNOR: Association Française de Normalisation
AOG: Addax and Oryx Group
BCP: Business Continuity planning
BIA: Business Impact Analysis
CCO: Cellule de crise opérationnelle
CCD : Cellule de crise décisionnelle
CDP : Clean Desk Policy
COBIT: Control objectives for information and related technology
CRAMM: CCTA Risk Analysis and Management Method
CRBF: Comité de la réglementation bancaire et financière
DAS: Direct Attached Storage
DRP : Disaster Recovery Plan
DRP: Disaster Recovery Plan
DSI: Direction des systèmes d'information
EBIOS: Expression des Besoins et Identification des Objectifs de Sécurité
EICNAM: Ecole d'ingénieur du Cnam
FMECA: Expression des Besoins et Identification des Objectifs de Sécurité
FTA: Fault Tree Analysis
GPL: Gaz et Produits liquéfiés
HAZOP: Hazard and Operability study
IEC : International Standard Community
IP: Internet Protocol
ISO : International Standard Organization
ITIL: Information Technology infrastructure Library
MAHARI: Méthode Harmonisée d'Analyse de Risques
MTD: Maximum Tolerable downtime
NAS: Network Attached Storage
NASD: National Association of stock dealers
NFPA : National Fire protect Association
OBSA: Oryx Bénin SA
OCTAVE: Operationally Critical Threat, Asset and Vulnerability Evaluation
PCA: Plan de continuité d'activité
PDCA : Plan-Do-Check-Act
RDM : Raw Device Mapping
RMF: Risk Management Framework
RPO: Recovery Point Objective
RTO: Recovery Time Objective
SAN : Stockage Area Network
SAN: Storage Area Network
SCSI: Small Computer System interface
SMCA : Système de management de la continuité des affaires
SPOF: Single Point of Failures
TCP: Transfert Control Protocol
VM : Virtual Machine
WAN: Wide Area Network

# Sommaire

<b>Introduction</b> .....	1
<b>1. Contexte</b> .....	2
1.1. Présentation de l'entreprise.....	2
1.2. Contexte de plan de continuité.....	6
<b>2. Etat de l'art: Continuité d'activité</b> .....	9
2.1. Définition .....	9
2.2. Terminologie.....	10
2.3. Principes.....	10
2.4. Piliers du PCA .....	11
2.5. Volets du PCA .....	14
2.6. Normes et standards.....	15
2.7. Démarche PCA .....	20
2.8. Infrastructures techniques .....	31
<b>3. Réalisation pratique</b> .....	37
3.1. Cadrage du projet DRP .....	37
3.2. Cartographie du SI .....	45
3.3. Cartographie des sinistres .....	55
3.4. Analyse d'impact .....	77
3.5. Analyse de risque.....	88
3.6. Conception de l'infrastructure optimisée.....	99
3.7. Implémentation des solutions techniques .....	100
3.8. Elaboration des plans et procédures.....	117
3.9. Retour d'expérience .....	118
<b>4. Bilan et alternatives</b> .....	123
4.1. Bilan projet .....	123
4.2. Bilan personnel .....	125
<b>Conclusion</b> .....	127
<b>Références</b> .....	128
▪ Bibliographie .....	128
▪ Webographie .....	128
▪ Index des figures .....	119
▪ Index des tableaux.....	130
<b>Annexe</b> .....	131
<b>Table des matières</b> .....	147

---

## Introduction

L'institut international de reprise après sinistre, estime que « *Lorsqu'elles n'y sont pas préparées, 43% des entreprises ferment au moment d'un sinistre majeur, et 29% de celles qui survivent, périssent dans les deux ans qui suivent* ». C'est conscient de cette réalité que le top management du groupe AOG (Addax and Oryx Group) a impulsé un projet de mise en place d'un plan de continuité d'activité, dans toutes les filiales du groupe. A cet effet, le projet DRP (Disaster Recovery Plan) a été initié au sein de la société OBSA (Oryx Bénin SA) avec pour objectif d'assurer la continuité des services informatiques et de Télécommunications, dans le cadre général du PCA (Plan de continuité d'activité) de ladite Société.

Au vue de la nécessité d'assurer une continuité d'activité, j'ai choisi d'intégrer mon projet de mémoire d'ingénieur dans le cadre du projet DRP, avec pour objectif spécifique, la conception de l'infrastructure optimisée. Pour atteindre cet objectif, je réaliserai dans un premier temps une cartographie des sinistres, qui servira de base à une étude d'impact sur l'activité, afin d'obtenir une matrice BIA (Business Impact Analysis). Ensuite, partant de la matrice BIA, j'effectuerai une analyse de risques pour ressortir un plan de réduction des risques sur la base des processus critiques; lequel plan servira de base à la conception de l'infrastructure optimisée.

Ce document représente mon mémoire d'ingénieur et s'organise en cinq chapitres déclinés successivement comme suit:

- Le contexte où je présente l'entreprise et plus spécifiquement, l'organisation du département où se déroule le travail de mémoire et ensuite, le contexte de plan de continuité d'activité.
- L'état de l'art dans lequel je présente une synthèse des connaissances relatives au plan de continuité d'activité, en insistant sur l'analyse d'impact, l'analyse de risque et les architectures techniques les plus usitées en la matière
- La réalisation pratique, qui est l'avant dernier chapitre où je présente au prime abord, le cadrage et la définition du projet DRP, ensuite, je décris formellement sa mise en œuvre, notamment le processus de conception de l'infrastructure optimisée.
- Le bilan qui est le dernier chapitre où je procède à une évaluation des objectifs atteints par rapport aux objectifs fixés, les difficultés rencontrées et les perspectives.



## **1. Contexte**

Mon projet de mémoire s'est déroulé au sein de la Direction des systèmes d'information du Groupe pétrolier AOG, où j'occupe actuellement le poste de Responsable Informatique de la filiale du Bénin depuis 05 ans, après avoir exercé durant quatre (04) années, la fonction d'administrateur système au sein de la même structure. Suite à mon admission à l'EiCnam (Ecole d'Ingénieur du Cnam) et à la présentation de mon projet de Mémoire, la Direction Générale a adhéré à ma demande de travailler à plein temps, sur le projet de mise en place du plan de continuité et de reprise d'activité informatique de l'entreprise, sous la coordination directe de l'administrateur DRP du Groupe.

Dans ce chapitre, je présente dans un premier temps, Oryx Bénin SA qui est l'entreprise où s'est déroulé mon projet de mémoire, ensuite je mets en exergue l'organisation et le fonctionnement de la Direction informatique, puis enfin, j'expose le contexte de plan de continuité de l'entreprise.

### **1.1. Présentation de l'entreprise**

L'objectif de cette présentation est de mettre en exergue, les différents secteurs d'activités, le chiffre d'affaire et l'organisation de la multinational AOG, tout en insistant particulièrement sur ORYX-BENIN qui en est l'une des filiales les plus importantes et où se déroule mon travail de mémoire.

#### **1.1.1. Profile du groupe AOG**

Le Groupe AOG a été créé en 1987 et s'est aujourd'hui positionné comme un acteur incontournable sur le marché de l'énergie en Afrique et au-delà. Ses activités couvrent cinq (05) secteurs principaux, que sont: Le négoce, l'exploration-production, le stockage et distribution, l'exploitation minière et la bioénergie.

Avec un chiffre d'affaire supérieur à trois (03) milliard de dollars, le Groupe compte plus de mille (1000) collaborateurs et rassemble une trentaine de nationalités différentes en Afrique et en Europe.

#### **1.1.2. Présence géographique**

Comme l'indique la carte illustrée par la figure n°1 ci-dessous, le groupe AOG dont le siège social est basé à Genève en Suisse est fortement présent en Afrique, mais également en Europe.

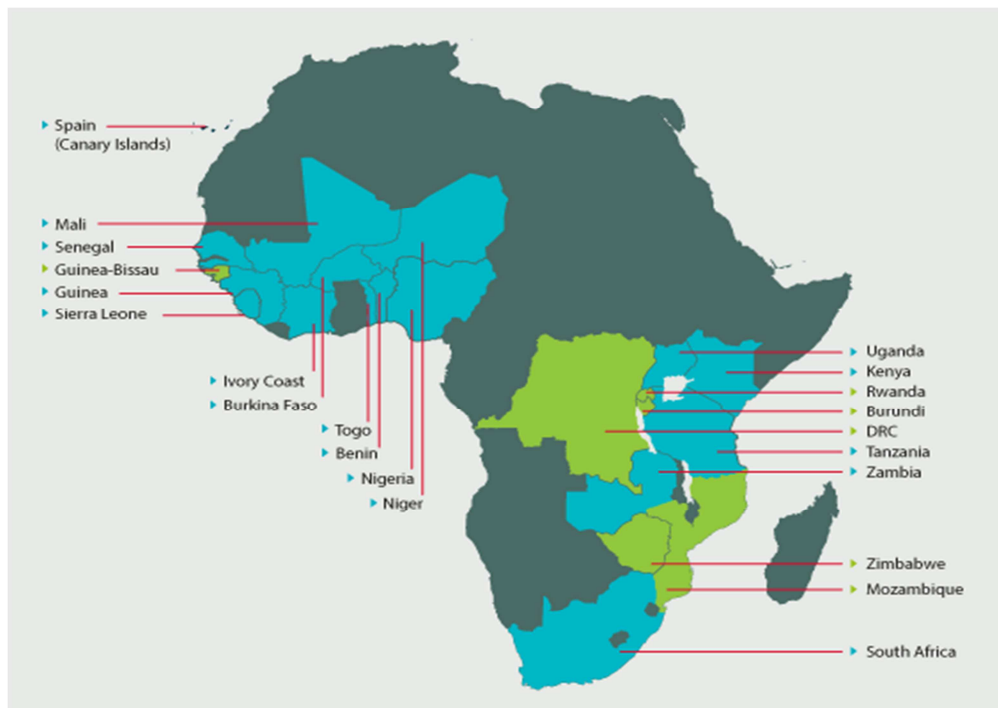


Figure n°1 : Présence géographique du Groupe AOG

### 1.1.3. Oryx Bénin SA (OBSA)

Créée le 02 janvier 1996, la société Oryx Bénin SA est spécialisée dans l'importation, l'exportation, le stockage, la distribution et le transport de produits pétroliers. Son capital social a évolué de 1.000.000 F CFA à la création à 500.000.000 F CFA en 2001 et 4.336.000.000 F CFA de 2004 à 2012. Les tableaux I et II ci-dessous, en présentent respectivement la fiche signalétique et la répartition du personnel.

RAISON SOCIALE	Oryx Bénin SA
SIEGE SOCIALE	Immeuble Maersk House- Domaine OCBN Ilot 531 parcelle B Cotonou
ADRESSE POSTALE	01 BP 464 RP Cotonou
TELEPHONE	(229) 21 31 07 70
FAX	(229) 21 31 18 26
E-MAIL	<a href="mailto:oryx.benin@aogltd.com">oryx.benin@aogltd.com</a>
DATE DE CREATION	02/01/1996
DATE DE DEMARRAGE	Novembre 1999
CAPITAL SOCIAL	1 300 000 000 FCFA
FORME JURIDIQUE	Société Anonyme
REGIME FISCAL	Droit commun
EFFECTIF PERSONNEL	102
ACTIVITE PRINCIPALE	Stockage et distribution des produits pétroliers
NUMERO D'IMMATRICULATION AU RCCM	20 0099-B
INSAE	2 957 192 546 292
IFU	3 200 700 018 111

Tableau I : Fiche signalétique d'OBSA

CATEGORIES PROFESSIONNELLES	EFFECTIFS		
	HOMMES	FEMMES	TOTAL
CADRES	6	1	7
AGENTS DE MAITRISE	16	4	20
TECHNICIENS SUPERIEURS	21	10	31
EMPLOYES	40	4	44
TOTAL	83	19	102

Tableau II : Répartition du personnel d'OBSA au 02-09-13

### 1.1.3.1. Le terminal pétrolier

En novembre 1999, ORYX BENIN a inauguré son terminal pétrolier et gazier dans le Port Autonome de Cotonou. Ces installations comprennent un quai privé de 250 m de long, sept réservoirs (bacs) de produits blancs et noirs pour une capacité totale de 55.000 m<sup>3</sup>, une sphère de gaz de 3.000 m<sup>3</sup> et un réservoir de GPL horizontal de 200 m<sup>3</sup>. La figure n°4 présente une vue partielle du terminal pétrolier d'ORYX-BENIN SA.



Figure n°2: Vue partielle du terminal d'OBSA

### 1.1.3.2. L'activité GPL

En 2000, ORYX a démarré son réseau de distribution de GPL (Gaz et produits liquéfiés) conditionné et passe de 1500 MT par an à près de 5000 MT, avec un réseau de distribution fort de trois cent soixante-dix (370) points de vente et environs cinquante mille (50.000) bouteilles de gaz en circulation.

### **1.1.3.3. L'activité Lubrifiant**

En 2003, ORYX s'est implanté sur le marché des lubrifiants où ses ventes sont en croissance constante (actuellement, plus de 30 MT par mois). Les lubrifiants ORYX sont certifiés ISO 9002.

### **1.1.3.4. Les stations-services**

En janvier 2004, ORYX a inauguré sa première station-service. A ce jour, le réseau de station-service de la filiale est composé d'une vingtaine de stations en gestion libre. La Figure n°3 ci-dessous, présente une vue partielle des produits et service d'OBSA.



Figure n°3: Vue partielle des produits et services d'OBSA

### **1.1.4. Organisation de la DSI (Direction des systèmes d'information)**

L'objectif stratégique de la DSI ainsi que les interactions entre la DSI et les services informatiques des filiales sont présentés ci-dessous.

#### **1.1.4.1. Objectif**

L'objectif premier de la DSI (Direction des Système d'information) est d'être en ligne avec les opérations, que ce soit lors de la recherche d'une solution de technologie de l'information, de sa planification, de sa mise en œuvre ou de son exploitation, tout en répondant à des critères d'économie, de performance et de sécurité, définis conjointement par les responsables métiers et les Responsables informatiques des filiales avec comme point focal, la création de synergie dans le Groupe AOG.

#### **1.1.4.2. Décentralisation**

La stratégie Informatique est décentralisée au niveau des filiales, sauf pour les systèmes et applications communs; ces derniers relevant de la sécurité, de la messagerie, des logiciels bureautiques, sans oublier l'architecture et le réseau qui sont communs.

### 1.1.4.3. Projets transversaux

Dans le cadre de la mise en œuvre de projets limités au périmètre de la filiale, le responsable informatique de la Filiale propose aux responsables métiers une équipe inter-division pour la préparation, la mise en œuvre et la maîtrise d'ouvrage du projet, sous l'autorité du DSI Groupe. Le recours à des experts dans le cadre d'un projet n'étant possible que si ce dernier nécessite le conseil d'un spécialiste ou une charge de travail que la Direction des systèmes d'information n'est pas en mesure de fournir.

### 1.1.4.4. Reporting

Le Responsable Informatique de la filiale rapporte au Directeur Général et collabore avec le DSI Groupe.

## 1.2. Contexte de plan de continuité

Dans sa stratégie globale, le groupe AOG, aborde la continuité d'activité en y définissant un cadre où sont présentées les attentes et implications relatives à la continuité des activités en son sein. Nous présentons ci-dessous ce cadre.

### 1.2.1. L'existant

Le groupe AOG dispose d'un référentiel interne en matière de règlements et de procédures, soulignant ce que le groupe attend de ses unités d'affaires et de ses employés dans divers domaines. Ce référentiel appelé PPM (Polices and Procédures Manuel) en ses chapitres n°3 et n°9, respectivement intitulé, « Gouvernance Groupe » et « Technologies de l'information » met un accent particulier sur la continuité et la reprise d'activité au sein du Groupe. Les figures n°4 et n°5 présentent respectivement un aperçu des chapitres n°3 et n°9 des PPM.

<b>Chapitre 3. GOUVERNANCE GROUPE (Tous)</b>
Règle 3.15 Continuité d'activité
Règle 3.16 Dénonciation (Compte-rendu confidentiel des employés)
Règle 3.17 Politique Anti-Corruption
Règle 3.19 Archivage des documents Groupe

Figure n°4: Extrait du PPM – Chapitre 3

<b>Chapitre 9. TECHNOLOGIE DE L'INFORMATION (Management)</b>
Règle 9.11 Plan de récupération de désastre
<b>Chapitre 9. TECHNOLOGIE DE L'INFORMATION (Tous)</b>
Règle 9.1 Organisation et stratégie
Règle 9.2 Gestion des applications-Licences de logiciels
Règle 9.3 Gestion des données
Règle 9.4 Support Utilisateur
Règle 9.5 Gestion de l'environnement technique
Règle 9.6 Gestion de la sécurité
Règle 9.7 Utilisation d'internet, des emails et de la messagerie instantanée
Règle 9.8 Continuité des systèmes
Règle 9.9 Intégrité des systèmes
Règle 9.10 Sauvegarde

Figure n°5: Extrait du PPM – Chapitre 9

Les règles 3.15 et 9.8 traitent respectivement de la continuité d'activité et de la continuité des Systèmes. Ci - dessous une synthèse de ces deux règles.

### 1.2.2. Synthèse

Avec pour objectif de garantir la disponibilité des systèmes et des traitements en cas de défaillance, pour le Groupe Addax et Oryx ces règles se déclinent en plusieurs clauses.

- A. La définition de l'infrastructure informatique et de télécommunication est telle qu'elle minimise le risque
- B. Le siège et les filiales doivent assurer la continuité de leurs systèmes dans des délais fixés à l'avance
- C. Chaque Directeur Général de Filiale définit en consultation avec son Service Informatique, les systèmes et les applications qui sont critiques et secondaires aux opérations.

- D. Les Directeurs Généraux de Filiale et le DSI Groupe déterminent les systèmes et applications, qui sont critiques aux opérations du groupe.
- E. Le responsable Informatique de la filiale en collaboration avec le DSI Groupe s'assure que chaque domaine technique ou fonctionnel critique ait un expert de premier recours et un spécialiste de second recours.
- F. Le DSI Groupe et le Responsable informatique de la filiale mettent en place l'infrastructure, les procédures de restauration de données et des accords de service avec des partenaires externes, pour la continuité des systèmes.**
- G. Le Responsable informatique de la filiale et le DSI Groupe testent le plan de continuité des systèmes périodiquement.

Le point « F » de la synthèse ci – dessous peut – être vu comme l'objectif in fine du travail objet du présent mémoire d'ingénieur, intitulé, « *De l'étude de risque à la conception de l'infrastructure optimisée dans le cadre d'un plan de continuité et de reprise d'activité informatique* ».

Il ressort des règles et exigences du PPM que mon travail de mémoire se déroule dans un contexte où la nécessité d'un plan de continuité est connue. Les objectifs à atteindre, ainsi que l'implication attendue de la Direction Générale en termes de continuité d'activité sont clairement définis dans le PPM. Par ailleurs, si ce dernier fournit les objectifs attendus d'un PCA, on n'y retrouve pas la réponse à la question « Comment atteindre ces objectifs ? ». C'est dire tout simplement qu'au jour aujourd'hui ORYX-BENIN SA ne dispose pas encore d'un plan de continuité et de reprise d'activité aligné sur les exigences normatives et de bonnes pratiques en la matière. L'étape à suivre de ce document aura donc pour objectif de présenter une synthèse des connaissances existantes en matière de plan de continuité d'activité.

## 2. Etat de l'art de la continuité d'activité

Dans un contexte mondial marqué par des catastrophes de tous genres, les entreprises font face à des situations de crise de plus en plus imprévues. Cela justifie l'affirmation de Didier Heiderich, je cite... « *Il n'y a que deux type d'entreprises: Celles qui sont en situation de crise et celles qui le seront.* ». Face à cette réalité, deux types de comportements peuvent s'observer:

- L'absorption du risque: Attendre patiemment l'avènement de la crise pour qu'intervienne la compagnie d'assurance, avec certes le dédommagement financier qui limitera les pertes financière, mais pas la baisse de productivité liée à la perte de clients, l'impact négatif sur l'image de l'entreprise et éventuellement les pénalités réglementaires pour non-respect d'obligations.
- La résilience: Prendre les dispositions nécessaires pour assurer la survie des activités de base de l'entreprise avant, pendant et après l'avènement d'une crise.

Quand on choisit d'assurer la pérennité de l'entreprise « la résilience », comme le groupe AOG, alors on s'engage dans un processus d'élaboration d'un PCA. Dans ce chapitre, sera présentée une synthèse des connaissances nécessaires à la mise en œuvre d'un plan de continuité d'activité.

### 2.1. Définition

Plusieurs définitions du plan de continuité d'activité fusent. Nous en présentons deux; celle du CRBF et celle de l'encyclopédie universelle Wikipédia:

« Le plan de continuité d'activité est un ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise, puis la reprise planifiée des activités». (CRBF 2004-02)

« Le plan de continuité et de reprise d'activité est un dispositif organisationnel et technique ayant pour objectif de limiter l'impact potentiel d'un sinistre, en permettant la reprise de l'activité, à plein régime ou en mode dégradé, au bout d'un certain temps, préalablement défini .» (Wikipédia)



## 2.2. Terminologie

La continuité d'activité dont la terminologie n'est pas encore normalisée, regorge de termes dont l'essentiel a été recensé dans le tableau III.

TERME FRANCAIS	TERME EQUIVALENT EN ANGLAIS
PCA: Plan de Continuité d'Activité	BCP: Business Continuity Plan
PRA: Plan de Reprise d'Activité	BRP: Business Recovery/Resumption Plan
PCO: Plan de Continuité des Opérations	COOP: Continuity of Operations Plan
PCC: Plan de Communication de crise	CCP: Crisis Communications Plan
PRII: Plan de réponse aux Incidents Informatiques	CIRP: Cyber Incident Response Plan
DRP: Disaster Recovery Plan	DRP: Disaster Recovery Plan
PIU: Plan d'Intervention d'Urgence	ERP: Emergency Response Plan

Tableau III: Terminologie

## 2.3. Principes

Le plan de continuité d'activité est la manifestation tangible de la continuité d'activité, dont la problématique se raccorde à celles de la gouvernance d'entreprise, du management des risques et de la gestion de crise. A ce titre, le PCA dont le concept est illustré par la figure n°6 doit – être conçu en vue de limiter les impacts adverses d'un sinistre sur l'activité d'une entreprise, assurer le fonctionnement des activités critiques pendant la crise et enfin, permettre un retour efficace à une situation nominale.

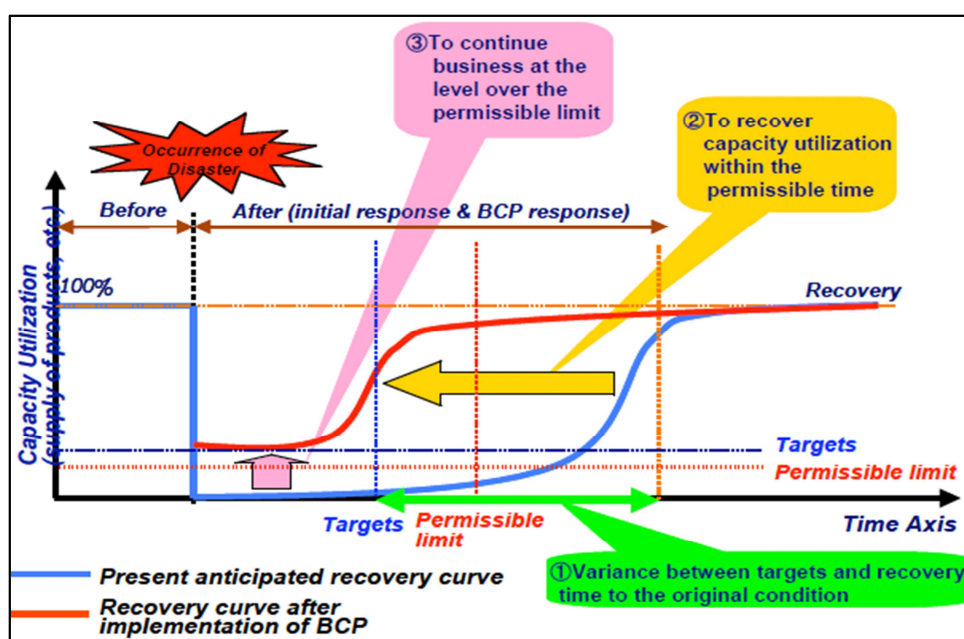


Figure n°6: Concept du PCA

Par ailleurs, Le PCA n'a pas vocation à répondre à des incidents d'exploitation ou de fonctionnement isolés, le PCA est l'ultime solution, lorsque toutes les mesures de prévention et de protection ont failli face à un sinistre. Le plan de continuité peut toutefois, contenir plusieurs plans propres à des services ou départements particuliers de l'entreprise.

## **2.4. Piliers du PCA**

Un PCA est basé sur quatre composants fondamentaux dont, l'ancrage ou l'inexistence conditionne la longueur, la complexité et la probabilité de réussite d'un projet de mise en œuvre de PCA. Nous présentons ci-dessous ces quatre piliers que sont l'organisation de crise, la stratégie de prévention et de préparation, la solution technique et le système documentaire.

### **2.4.1. L'organisation de gestion de crise**

C'est le dispositif de management de la crise et de pilotage de la mise en œuvre du PCA. Concrètement il s'agit de cellules constituées d'acteurs disposant de pouvoirs de décisions et de capacité de coordination. Le référentiel BP Z74-700 de l'AFNOR présente la CDD (cellule de crise décisionnelle) comme étant l'organe principal de l'organisation de crise. Essentiellement constituée d'acteurs à fort pouvoir de décision (Directeurs), elle est chargée d'arbitrer les décisions stratégiques, de gérer les imprévus, de financer l'urgence et de coordonner la politique de communication en s'appuyant sur les trois cellules suivantes:

- La cellule de crise opérationnelle  
C'est la cheville ouvrière du PCA; cette cellule constituée des équipes métiers et de support intervient à tous les niveaux opérationnels du PCA.
- La cellule de communication  
Cette cellule se charge de la définition et de la mise en œuvre de la politique de communication interne et externe.
- La cellule d'expertise  
Elle est chargée d'analyser et de capitaliser l'expérience

La Figure n°7, ci-dessous présente un schéma d'organisation de crise mettant en évidence, les interactions entre les différentes cellules.

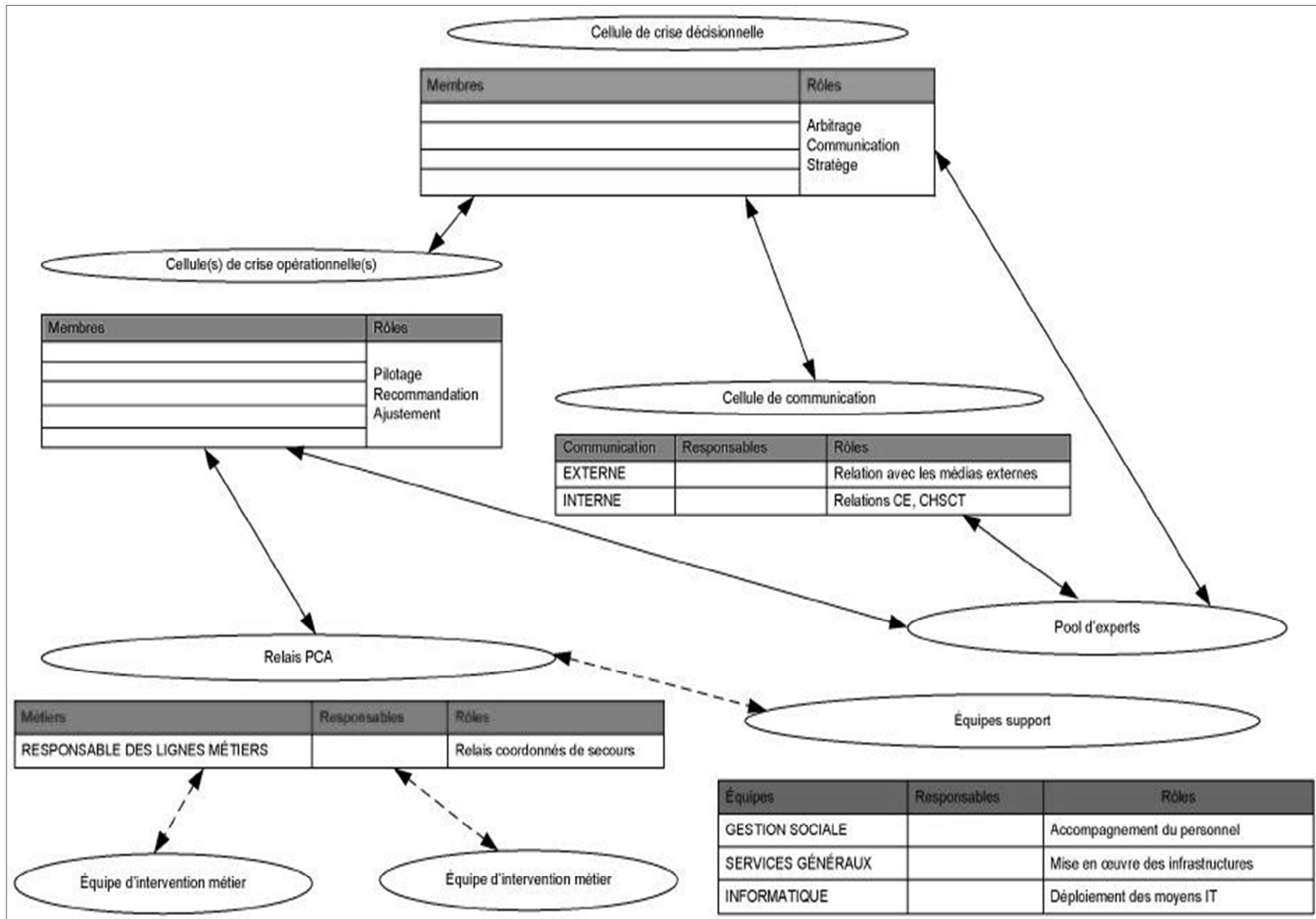


Figure n°7: Schéma de crise

#### **2.4.2. Le système documentaire**

Le système documentaire est le principal référent en cas de crise. Robert Bergeron du cabinet BCP–Expert recommande que tout en étant à jour, testée, connue des potentiels utilisateurs et accessible en toute circonstance, la documentation du PCA soit gérée par un logiciel spécialisé, tandis que le référentiel BP Z74-700 de l'AFNOR détail un peu plus ce volet en recommandant de baser la gestion de la documentation du PCA sur les trois critères de confidentialité, criticité et accessibilité. Elle recommande à cet effet d'étudier:

- Les informations, procédures, modèles types à mettre à disposition des services/acteurs
- Le nombre de documents PCA à produire ou déjà produits
- Les droits d'accès
- Les modes de support de stockage

Ensuite, tenant compte des exigences d'accessibilité aux informations et la limitation des contraintes de l'organisation existante, utiliser les outils bureautiques (Word, Excel, access...etc.) ou choisir un logiciel de gestion de la documentation d'un PCA.

#### **2.4.3. Stratégie de prévention et de préparation**

Il s'agit de la définition formelle des mesures de prévention, détection et protection face à un sinistre ou une crise. La stratégie de prévention et de préparation doit définir les mesures mises en place par l'entreprise pour renforcer son état de préparation à faire face à un sinistre ou une crise. Elle englobe:

- Les mesures de détection de sinistre,
- Les mesures de protection contre les menaces
- Les mesures de réduction de l'exposition aux événements redoutés
- Les mesures de colmatage des vulnérabilités

Les bonnes pratiques recommandent d'intégrer ces mesures la stratégie globale d'entreprise.

#### **2.4.4. La solution technique de continuité**

La solution technique du PCA est l'ensemble constitué des éléments de secours du système d'information, des infrastructures, des moyens et des ressources, permettant

de maintenir active la cible fonctionnelle en cas d'avènement de crise ou de sinistre impactant les activités de l'entreprise. On distingue trois types de solutions de secours que sont:

- la solution de secours des moyens informatiques,
- la solution de secours de moyens de production
- le secours de ressources humaines.

Il importe de noter que dans les secteurs tertiaires (banque, assurance, service, télécommunications, etc.) le système d'information est l'outil de production.

## 2.5. Volets du PCA

Un plan de continuité d'activité tel qu'illustré à la Figure n°8, est constitué essentiellement de trois grandes parties, qui rassemblent l'ensemble des mesures visant à assurer face à différents scénarios de crise et de sinistres, le maintien des activités essentielles de l'entreprise.

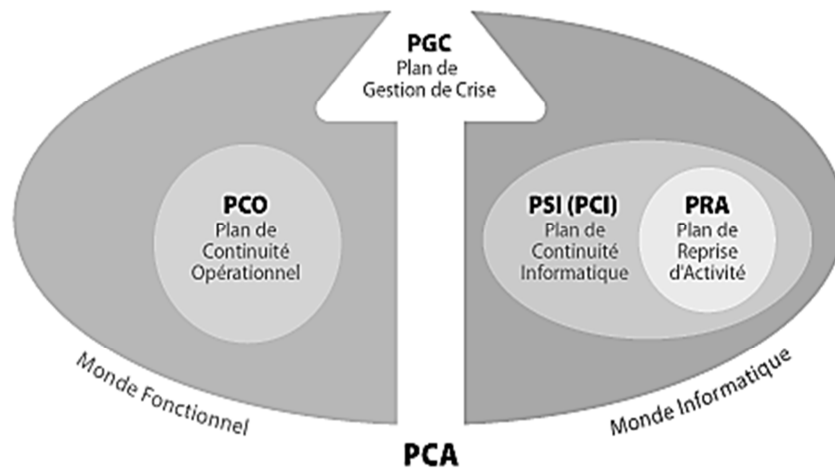


Figure n°8: volet du PCA

- Le **PCO** (Plan de continuité opérationnelle): Le Plan de Continuité opérationnelle évalue les différents scénarios liés aux activités métiers critiques, puis définit et met en œuvre les moyens préventifs adaptés.
- Le **PCI/PSI** (Plan de Continuité Informatique): Le **PSI** (Plan de Secours Informatique) ou **PCI** (Plan de Continuité Informatique) a pour but d'assurer 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 constitué d'une analyse des risques et de leurs impacts, d'une stratégie composée de mesures préventives et curatives puis des procédures de tests afin de s'assurer de la validité technique du PCI/PSI.

- Le PGC (Plan de Gestion de Crise): Il s'agit du plan qui 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 acquise de chacune des crises précédentes, permettant ainsi, une amélioration de la vision prospective de la gestion de crise.

## **2.6. Normes et standards**

Dans ce sous – chapitre, sont présentés les différentes normes et standards traitant peu ou prou de la continuité d'activité.

- **ISO 22301:2012**

C'est la norme par excellence de la continuité d'activité. Elle spécifie les exigences pour planifier, déployer, mettre en œuvre, exploiter, surveiller, maintenir et améliorer en permanence un système de gestion documenté pour permettre de réduire la probabilité d'occurrence d'un événement désastreux, s'y préparer, intervenir et récupérer à la suite de la survenance d'incidents perturbateurs quels qu'ils soient. C'est exigences sont structurées au sein d'une série de clauses. La mise en œuvre d'un SMCA (système de management de de la continuité des affaire) y est traité au niveau de la clause N°8 intitulée: Gestion des opérations, déclinée comme suit: Analyse d'impact - Analyse de risque - Stratégie de continuité de l'activité - Procédure de la continuité de l'activité - Tests et exercices.

- **ISO/IEC 27031:2011**

Cette norme présente les concepts et principes relatifs à la continuité des TIC (Technologies de l'information et de la Communication). Elle permet

également à l'organisme de mesurer, de manière méthodique et reconnue, les paramètres de performance qui se rapportent à la mise en état des TIC dans le cadre de la continuité des activités et recommande à cet effet d'implémenter la méthode PDCA (Plan Do Check Act).

- **ISO/IEC 24762 : 2008**

Cette norme propose des orientations relatives au secteur des technologies de l'information et de la communication (TIC), dans le cadre de la gestion de la continuité opérationnelle en cas de sinistre. Elle présente les lignes directrices pour une bonne exploitation du système de management de la sécurité de l'information (SMSI) sous ces aspects de disponibilité de l'information pour la gestion de la continuité des opérations en temps de crise. La norme «ISO/IEC 24762 » met un accent particulier sur la prestation de service en matière de continuité d'activité.

- **ISO/PAS 22399:2007**

Cette norme établit le processus, les principes et la terminologie de la préparation aux incidents et à la gestion de la continuité opérationnelle. En somme, elle intègre les processus de planification et de gestion permettant d'assurer de façon proactive les objectifs de continuité d'activité au sein d'une organisation

- **ISO/IEC 27002: 2005**

Cette norme dont le contenu technique est identique à celui de la norme ISO/IEC 17799: 2005 traite de la démarche et des principes pour la préparation, la mise en œuvre, l'entretien et l'amélioration de la gestion de la sécurité au sein des organismes. Elle traite tout particulièrement de la continuité d'activité en son article N°14 sommairement présenté ci-dessous:

En bref, le chapitre n°14 de la norme ISO/IEC 27002 décrit les mesures à adopter pour la gestion d'un plan de continuité de l'activité visant à réduire le plus possible l'impact sur l'organisme et à récupérer les actifs informationnels perdus, notamment à la suite de catastrophes naturelles, d'accidents, de pannes de matériel et d'actes délibérés.

- **HB 221 :2004**

Cette norme présente le cadre général et les processus fondamentaux qui devraient être inclus dans un processus global de continuité de l'activité, elle est constituée de deux parties. La première partie qui propose une définition du management de la continuité d'activité en décrivant une démarche progressive de sa mise en place et la deuxième partie qui définit un cadre de management de la continuité des affaires.

- **BS 25999**

BS 25999 est la norme de l'organisme British Standards Institute (BSI) relative au management de la continuité d'activité. Elle est constituée de deux parties dont la première est un guide établissant les processus, les principes et la terminologie pour le Management de la continuité des activités tandis que la deuxième partie spécifie les exigences de la mise en place, d'exploitation et d'amélioration d'un système de management de la continuité des activités (SMCA).

- **BP Z74-700**

C'est le référentiel de l'association française de normalisation (AFNOR) de bonnes pratiques, sur les plans de continuité d'activités. Il aborde quatre grands thèmes que sont:

- Remontées d'incidents, évaluation et alerte
- Cellule de gestion de crise
- Plan de continuité informatique et télécoms
- Maintenance en condition opérationnelle

Ce référentiel présente un schéma des procédures de mise en œuvre d'un PCA à quatre niveaux, ci-dessous illustré par la figure n°9.





Figure n°9: Etapes de mise en œuvre d'un PCA

- **Standard international ITIL**

ITIL (Information Technology infrastructure Library) est une collection d'ouvrages qui recense, synthétise et détaille les meilleures pratiques portant sur la gestion des services liés aux technologies de l'information. ITIL aborde la continuité d'activité dans son livre consacré à la fourniture des services, qui traite de la planification et l'amélioration à long terme de la fourniture de services liés aux technologies de l'information. On y présente l'ISTM (IT service continuity management) comme partie intégrante, soutenant le processus de BCM (business continuity management) et fournissant l'infrastructure IT, prédéterminée et validée, nécessaire à la continuité de l'activité suite à une interruption de service due à une simple panne d'une application ou d'un système, à la perte des locaux.

- **ASIS SPC.1-2009**

Ce référentiel Américain propose une approche globale du système de gestion de la résilience organisationnelle, en spécifiant les exigences en matière de sécurité, préparation, intervention, atténuation, continuité des affaires/opérations et reprise d'activité en cas d'urgence, de crise ou de catastrophe.

- **NFPA 1600 – 2007**

Ce référentiel développe différents aspects des plans de continuité, notamment la Gestion (administration, coordination, évaluation des plans...) et les éléments constitutifs du plan (évaluation de risque, planification, communication, avertissement, formation, exercices, évaluation, actions correctives, législation, prévention des incidents...etc.).

- **AS/NZS 5050**

Ce référentiel Australo-Néo-Zélandais, met en évidence les liens entre la continuité d'activité et la gestion des risques. En adoptant une approche basée risque, elle inscrit fermement la continuité d'activité dans le processus de gestion de risques. Elle propose une approche proactive pour le contrôle des risques qui influent sur l'ampleur et la probabilité d'événements potentiellement perturbateurs.

- **SS540**

Ce référentiel singapourien de continuité des activités établit le cadre d'analyse, de mise en œuvre de stratégies, des processus et des procédures. Elle met l'accent sur la résilience et la protection des biens essentiels, l'homme, l'environnement, les immobilisations incorporelles et physiques.

- **CSA Z1600**

Ce référentiel canadien établit un ensemble de critères pour la gestion du programme d'urgence et de continuité des activités en fournissant les éléments d'un processus d'amélioration continue pour le développement, la mise en œuvre, la maintenance et l'évaluation desdits programmes.

- **Lignes directrices du PCA du Gouvernement Japonais**

Ce standard japonais, établit les orientations pour réduire l'impact des catastrophes et améliorer le cas échéant les réponses. Il a l'avantage d'aborder de façon succincte les concepts de base de la continuité d'activité, mais n'aborde pas les aspects relatifs à la continuité des TIC et est dédiée aux entreprises japonaises.

- **NASD 3510/3520**

NASD 3510 et NASD 3520 sont des règles de la série 3500 du (NASD) National Association of Stock Dealers, validée par la Security and exchange commission. Cette série de règles a pour objectif d'imposer aux membres du NASD la mise en place des plans et des procédures d'intervention d'urgence. NASD 3510/3520 est en bref une incitation à la mise en place de plan de continuité et un bel exemple des exigences réglementaire en la matière.

- **NIST SP 800-34**

C'est un guide de planification d'urgence pour les systèmes d'information fédéraux, qui fournit des instructions, des conseils et des considérations en matière de planification d'urgence des systèmes d'information fédéraux. NIST SP 800-34 couvre l'élaboration du plan d'urgence en se focalisant sur les TIC; à ce titre, il n'aborde qu'implicitement la continuité des opérations.

## **2.7. Démarche PCA**

La clause N°8 de la norme ISO 22301 intitulée « Gestion des opérations » identifie cinq (05) phases successives comme étant fondamentales dans la mise en œuvre d'un PCA; il s'agit respectivement de l'analyse d'impact sur l'activité, l'analyse de risque, la stratégie de continuité de l'activité, les procédures de continuité et les tests. Chacune de ces étapes est présentée ci-dessous.

### **2.7.1. Analyse d'impact sur l'activité**

L'analyse d'impact est la phase la plus sensible dans la mise en œuvre d'un PCA, en ce sens que, de son degré d'exigence dépend la fiabilité du PCA.

#### **2.7.1.1. Définition**

L'analyse d'impact sur l'activité peut être définie comme étant la détermination des impacts sur une entreprise d'une interruption d'activité faisant suite à un sinistre. Les impacts à considérer devraient porter aussi bien sur les pertes financières que sur l'image de l'entreprise, ses obligations réglementaires et juridiques, ses contraintes sociales et organisationnelles. (Source AFNOR)

### 2.7.1.2. Etapes de l'analyse d'impact

Se basant sur les scénarios de sinistres retenus, l'analyse d'impact s'articule autour des neuf (09) points suivants:

- Identification des activités: Via un découpage des activités de l'entreprise en plusieurs niveaux, on procède à une identification des activités critiques et ceci en collaboration avec les responsables métiers.
- Estimation des impacts financiers et opérationnels: Les impacts financiers sont évalués par jour en termes de montant ou par mesures qualitatives échelonnées ou notées, tandis que les impacts opérationnels sont évalués suivant une grille d'analyse élaborée de commun accord avec les responsables métiers.
- Identification des processus critique: Cela revient à établir, sur la base des activités essentielles et l'estimation des impacts financiers et opérationnels, un classement final des activités pour en déduire les processus critiques.
- Détermination des configurations: Pour chaque processus critique, on établit le MTD (Maximum Tolerable Downtime) qui est La durée maximale tolérable d'interruption de l'activité et les priorités de relance des activités en tenant compte des impacts financiers et opérationnels ainsi que du facteur temps. En effet, comme le montre la figure n°10, pour certaines activités, l'impact monte plus ou moins vite avec la durée de la panne.

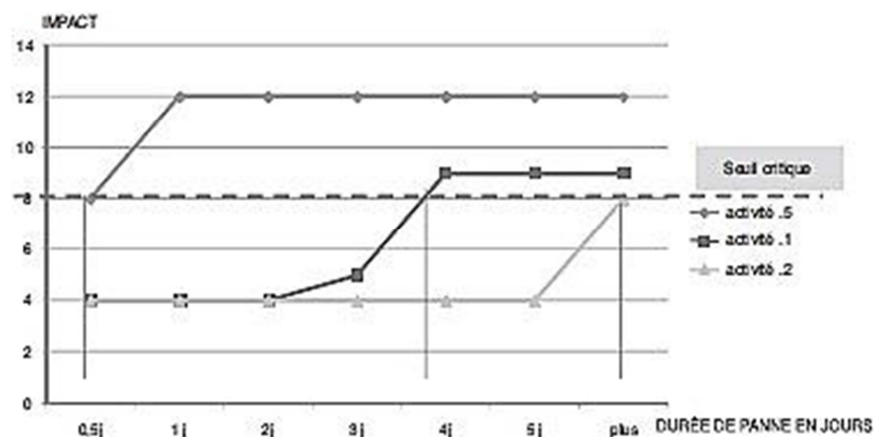


Figure n°10: Impact du facteur temps

- Systèmes et applications informatiques critiques : Partant des processus critiques, on détermine les applications et moyens informatiques critiques en tenant compte de la situation géographique des moyens techniques et de la virtualisation des servers.
- Ressources humaines et autres ressources critiques : On élabore en collaboration avec les responsables métiers, une liste prenant en compte les compétences des ressources humaines ainsi que la liste détaillée des moyens indispensables pour travailler.
- Détermination des paramètres de reprise : Pour chaque groupe d'applications et de système correspondant à une activité critique, on détermine les paramètres de reprise que sont :
  - RTO (Recovery Time Objective): C'est le délai qui s'écoule entre la perte des moyens à cause du sinistre et leur récupération dans un état acceptable. Il est estimé sur la base d'indicateurs fourni par les utilisateurs.
  - WRT (Work Recovery Time): C'est la période qui suit le retour de l'informatique, caractérisé par le travail de mise à niveau des données. Cette durée est également estimée sur la base des indicateurs fournis par les utilisateurs
  - RPO (Recovery Point Objective): C'est le temps qui sépare le sinistre de la dernière sauvegarde utilisable. Ce paramètre est imposé par les choix techniques qui ont été faits pour se prémunir d'un sinistre et reste dépendant de la fréquence des sauvegardes.

La Figure n°11 ci-dessous présente une chronologie de crise mettant en exergue les paramètres RTO et RPO.

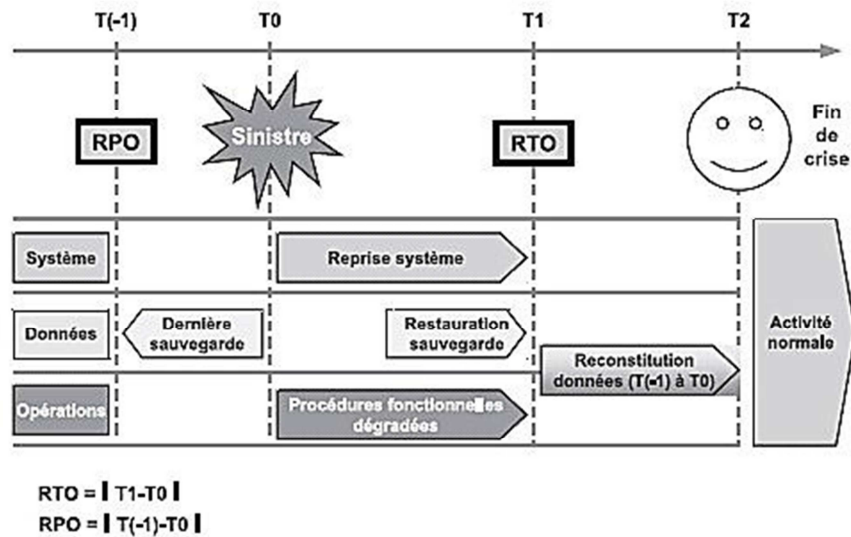


Figure n°11: Chronologie de crise

- Procédures de secours: Ce sont les procédures de fonctionnement en mode dégradé des processus critiques. On procède tout d'abord à une collecte et à l'évaluation des procédures existantes, puis ensuite à l'élaboration des procédures manquantes.
- Documentation de l'analyse d'impact sur les activités: Le document récapitulatif issu des différentes étapes de l'analyse d'impact sur les activités sera conservé dans un système documentaire adapté et à la disposition des auditeurs.

A l'issue de l'analyse d'impact sur l'activité, on aura déterminé les objectifs de récupération et de reprise (RPO et RTO), Les ressources clés, les impacts des sinistres sur l'activité, les points de défaillance unique (SPOF) et les contraintes.

## 2.7.2. Analyse de risques

L'analyse de risque est l'étape qui suit celle de l'analyse d'impact avec pour objectif, l'élaboration du plan de réduction des risques. C'est une étape très importante dans une démarche de mise en œuvre de PCA.

### 2.7.2.1. Définition

L'analyse de risque se définit comme étant un Processus systématique et exhaustif d'identification et d'estimation des risques (Source BS 25999-1).

### 2.7.2.2. Mesure du risque

Le risque se mesure par la multiplication de deux critères que sont la fréquence ou probabilité et la gravité ou impact ; la fréquence exprimant la probabilité de survenance du risque et la gravité, l'importance des impacts envisagés en cas de survenance du risque. Ce qui se traduit par la formule:

$$\text{Risque} = \text{Criticité} = \text{Fréquence} \times \text{Gravité} = \text{Probabilité} \times \text{Impact}$$

Les dispositifs de protection et de prévention diminuent respectivement l'impact en cas de survenance et la probabilité de survenance des risques. La mise en œuvre de ces mesures induit les notions de risque net et risque brut en ce sens que le risque net correspond au risque brut affecté de mesures de protection et ou de prévention. Il en ressort les formules de calcul suivantes :

$$\text{Criticité nette} = \text{criticité brute} / \text{Maîtrise}$$

$$\text{Criticité nette} = \text{Criticité brute} \times \text{Gravité nette}$$

$$\text{Criticité nette} = (\text{Fréquence brute} / \text{prévention}) \times (\text{Gravité brute} / \text{Protection})$$

La figure n°12, ci-dessous, présente une matrice d'évaluation de risque mettant en évidence l'effet de la protection et de la prévention.

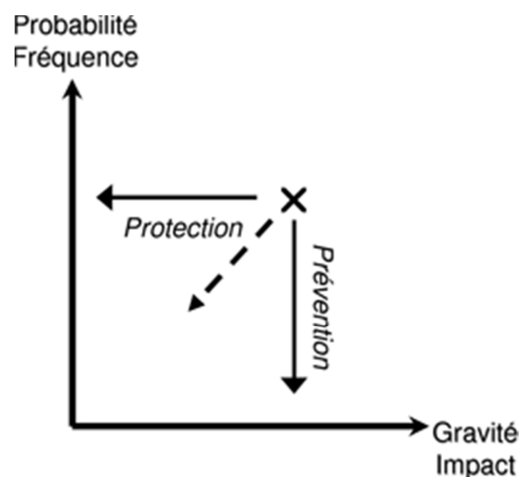


Figure n°12: Matrice de risque

### 2.7.2.3. Etapes de l'analyse de risque

L'analyse de risque constitue une étape primordiale de la mise en œuvre d'un PCA. Elle s'effectue en quatre (04) étapes successives. Nous présentons ci-dessous les étapes de réalisation d'une analyse de risque.

- Identifier les risques qui pèsent sur les processus et ressources critiques : L'outil utilisé à cette étape est la « typologie de risque et sinistre » qui est un recensement des principaux risques qu'on adaptera au contexte de l'entreprise.
- Evaluation de la probabilité d'occurrence et l'impact potentiel des risques : A cette étape, deux outils s'avèrent indispensables; la grille d'évaluation des impacts des sinistres qui peut – être construit à partir de modèles classiques suivant les enjeux des activités de l'entreprise et l'échelle d'évaluation des risques qui permet d'évaluer le couple [probabilité, impact] pour chaque risque afin d'en déduire la sévérité nette, en fonction de la sévérité brute et les mesure de protection et de prévention mises en œuvre.
- Définir la stratégie de gestion des risques : Quatre possibilités s'offrent à ce niveau, en termes de stratégie:
  - Suppression du risque: Cela revient à contourner ou éviter le risque.
  - Transfert du risque: La meilleure application en la matière est le recours aux assurances.
  - Acceptation du risque: Stratégie applicable aux risques d'impacts potentiellement faibles.
- Définir les plans de réduction des risques: C'est à cette étape de l'analyse de risque, qu'on procède à la détermination des actions nécessaires à la réduction ou à l'élimination des risques, des SPOF et à la hiérarchisation du traitement des risque en fonction des dépendances.

#### **2.7.2.4. Méthode d'analyse des risques**

Il existe sur le marché plusieurs outils méthodologiques d'analyse de risque, allant des plus spécialisés au plus généralistes. Nous présentons ici les démarches d'investigation en matière d'analyse de risque et les outils méthodologiques les plus connus du marché.



### 2.7.2.4.1. Démarches d'investigation

Il existe deux grands types de démarches d'investigation pour l'analyse des risques que sont la démarche inductive illustrée par la figure n°13, qui procède des causes vers les effets et la démarche déductive illustrée par la Figure n°14, qui procède des effets vers les causes. C'est deux démarches sont complémentaires et peuvent être associées dans le cadre d'une analyse de risque.

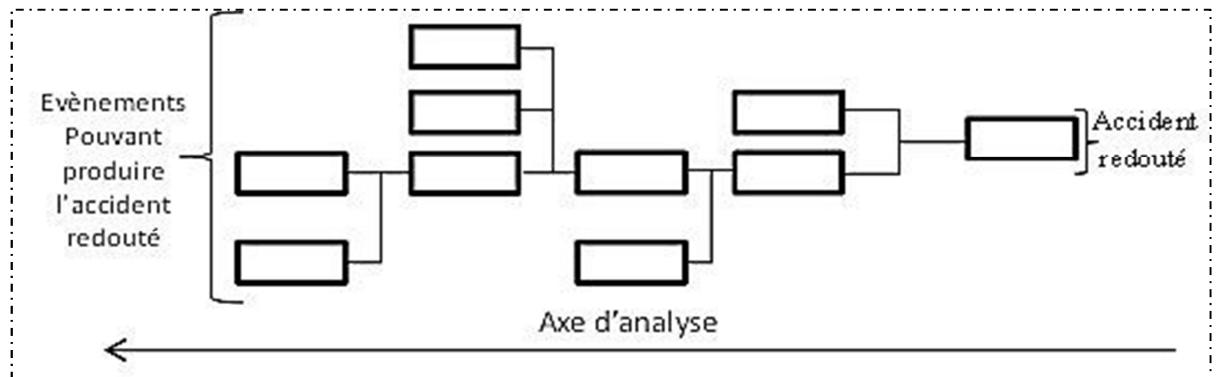


Figure n°13: Démarche inductive

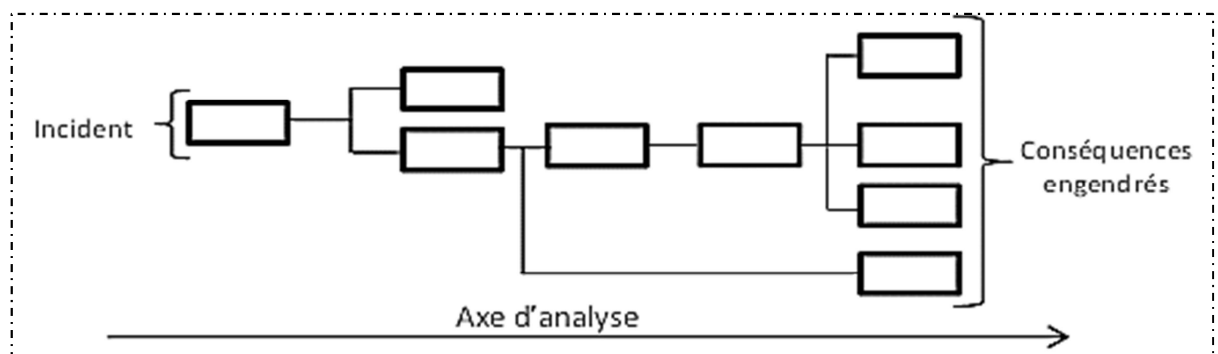


Figure n°14: Démarche déductive

### 2.7.2.4.2. Outils méthodologiques

Il existe sur le marché plusieurs méthodes classiques d'analyse des risques. Nous en présentons ci-dessous les principales:

- **COBIT** (Control objectives for information and related technology)

C'est une méthode de maîtrise de gouvernance et d'audit de systèmes d'information suivant une démarche qui s'inscrit dans une dynamique

d'amélioration continue, de généralisation de la pratique d'audit et garantissant la gestion des risques suivant une méthodologie orientée vers les processus métiers (business).

- **CRAMM** (CCTA Risk Analysis and Management Method)

C'est une méthode d'analyse et de maîtrise des risques liés aux systèmes d'information. Entièrement conforme aux exigences des normes BS7799 et ISO 27001. La méthode propose une démarche basée sur l'identification de l'existant, l'évaluation des menaces et des vulnérabilités et le choix de contres mesures.

- **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité)

La méthode EBIOS permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Sa démarche consiste en l'étude du contexte, l'expression de besoins de sécurité, l'étude des menaces, l'expression des objectifs de sécurité et la détermination des exigences de sécurité.

- **FMECA** (Failure Modes, Effects and Criticality Analysis)

Cette méthode adopte essentiellement une démarche inductive, qui consiste à identifier au niveau d'un système ou d'un de ses sous-ensembles, les modes potentiels de défaillance de ses éléments, leurs causes, leurs effets et une évaluation de la criticité de ces modes de défaillance. C'est la méthode par excellence en matière de sûreté de fonctionnement.

- **FTA** (Fault tree Analysis)

C'est une méthode ayant pour objectif la détermination de la raison initiale d'apparition d'un évènement non désiré et la probabilité que celui-ci survienne. Elle adopte une démarche déductive et est basée sur un modèle graphique (diagramme logique).

- **RMF** (Risk Management Framework)

C'est un cadre de gestion de risques fournissant un processus continu et structuré d'analyse des risques en 05 étapes tel qu'illustré à la Figure n°15 ci-dessous.

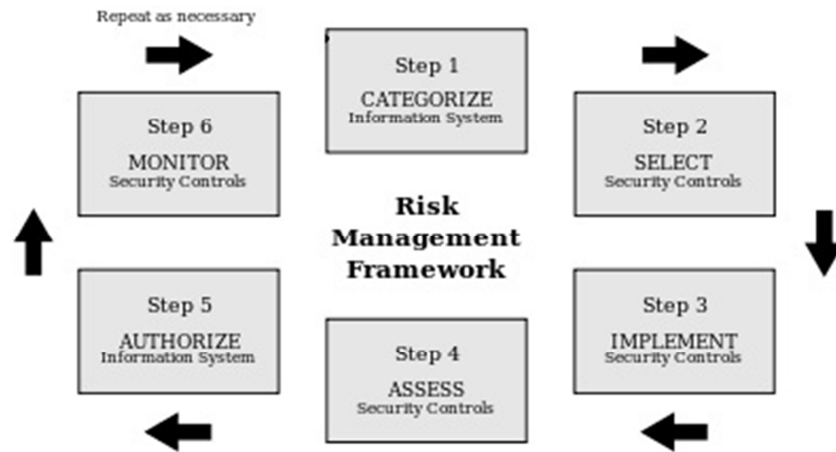


Figure n°15: Cadre RMF

- **CORAS**

C'est un cadre de gestion de risque basé sur l'intégration entre les méthodes d'analyse de risque et les méthodes de spécification avec un outil adaptable d'analyse de risque.

- **HAZOP (Hazard and Operability study)**

C'est une des méthodes les plus utilisées pour l'analyse des risques industriels. Son intérêt est l'identification et l'évaluation des situations pouvant représenter un risque pour le personnel ou les équipements, et le déploiement des moyens (procédés, équipements) de prévention adéquats.

- **ITIL**

ITIL propose une méthodologie en 09 étapes qui est un récapitulatif des bonnes pratiques en matière d'analyse de risque.

- **MAGERIT**

C'est la méthodologie d'analyse et de gestion des risques des Systèmes d'information utilisée par l'Etat Espagnol.

- **MEHARI** (Méthode Harmonisée d'Analyse de Risques)

C'est la méthode remplaçante de « MARION ». Elle permet l'appréciation des risques au regard des objectifs de sécurité et offre un cadre de contrôle de gestion de la sécurité en trois phases qui sont: Le plan stratégique de sécurité, le plan opérationnel de sécurité et le plan opérationnel d'entreprise.

- **OCTAVE** (Operationally Critical Threat, Asset and Vulnerability Evaluation)

Cette méthode a pour but de permettre à une entreprise de réaliser par elle-même, l'analyse des risques de leur SI, sans aide extérieure.

### 2.7.3. Stratégie de continuité

L'analyse de risque et d'impact sur l'activité ayant permis de fixer les exigences de continuité d'activité, on aborde la phase de définition des dispositifs, méthodes et moyens alternatifs qui permettront à l'entreprise de continuer son activité en cas de sinistre. C'est également à cette étape que s'opère tel qu'illustré à la Figure n°16, l'alignement stratégique du PCA. Cette phase s'articule autour des quatre (04) points suivants:

- Identification des enjeux majeurs : Ces enjeux peuvent être d'ordre économique, concurrentiel ou autres, mais intimement liés à la mission, aux valeurs, à la stratégie et aux objectifs de l'entreprise.
- Expression des exigences de continuité: L'expression des exigences de continuité se rattache aux obligations réglementaires du domaine d'activité de l'entreprise en matière de continuité d'activité, les seuils d'impacts de tolérance métiers.
- Hiérarchisation des scénarios de risques à couvrir : C'est à cette étape qu'on hiérarchise suivant leur niveau de criticité, les différents scénarios de risques. Les scénarios classiques traitent en général de la destruction ou indisponibilité des bâtiments, indisponibilité du SI, défaillance d'un prestataire, indisponibilité du personnel.

- Stratégies de reprise : L'élaboration de la stratégie de reprise revient à choisir selon les scénarios de crise précédemment retenus, des solutions technique et fonctionnelle de secours. C'est à cette étape qu'on conçoit l'architecture optimisée, pour une effectivité de la continuité d'activité en cas de sinistre.

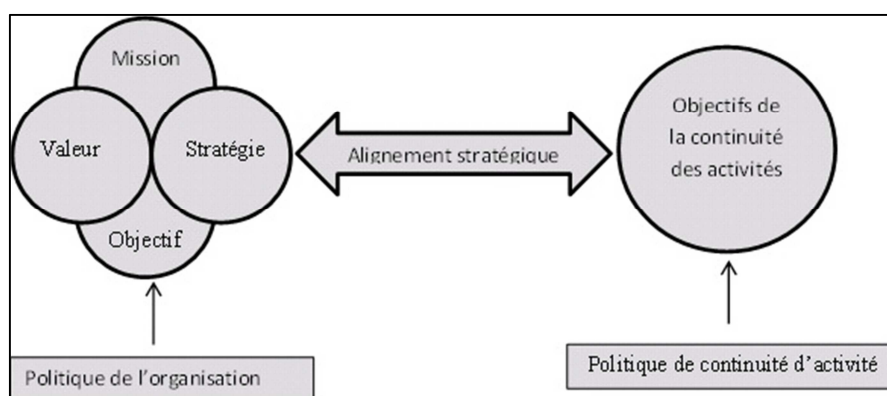


Figure n°16: Alignement stratégique du PCA

#### 2.7.4. Procédures de continuité

C'est la partie du PCA consacrée à la rédaction des plans et à la documentation des procédures et dispositions en vue d'assurer la continuité des activités et la gestion d'incidents perturbateurs. C'est à cette étape qu'on formalise les différents volets du PCA que sont:

- Le plan de gestion de crise (PGC)
- Le plan de continuité des opérations (PCO)
- Le plan de continuité informatique (PCI) et le plan de reprise d'activité (PRA)

#### 2.7.5. Tests

La phase de test a pour objectif de déceler les incohérences et insuffisances du dispositif de continuité d'activité, tout en procédant aux améliorations des procédures en vigueur. C'est également à cette phase que sont formés les acteurs du PCO à leur rôle de maintien en condition opérationnelle du PCA.

## 2.8. Infrastructures techniques

La mise en place des solutions techniques de continuité d'un PCA passe par la conception de l'infrastructure optimisée; c'est-à-dire, tenant compte des exigences techniques issues du PCA. Pour ce faire, il convient de faire appel à différentes techniques, choisir une typologie voire une topologie. Nous présentons ci – dessous, l'essentiel des techniques, la typologie et la topologie des architectures les plus usitées en matière de continuité du système d'information.

### 2.8.1. Les techniques

La mise en œuvre des architectures et autres infrastructures de continuité fait appel à des techniques quelque peu particulières. Nous présentons dans ce chapitre les techniques les plus usitées en la matière.

#### 2.8.1.1. La mise en Cluster

La mise en cluster telle qu'illustrée par la figure n°17 permet à plusieurs servers de s'interconnecter afin de s'afficher comme s'il s'agissait en réalité d'un seul server.

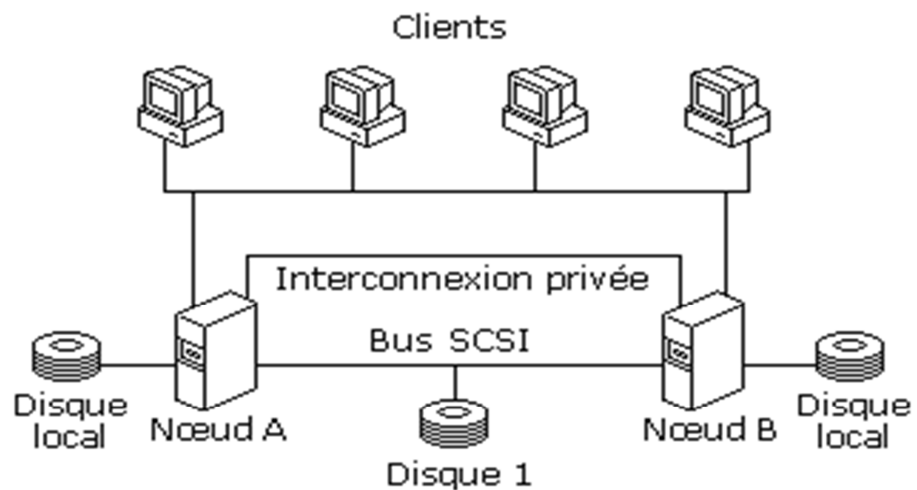


Figure n°17: Cluster de server

La mise en cluster permet de profiter d'un certain nombre de fonctionnalités que sont:

- Tolérance aux pannes : La tolérance aux pannes désigne une méthode de conception permettant à un système de continuer à fonctionner, éventuellement en « mode dégradé », au lieu de tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement.
- La répartition de charge: La répartition de charge permet de distribuer dynamiquement le trafic d'informations entre plusieurs servers (perçu comme un seul server de l'extérieur) sur lesquels tourne la même application. Le répartiteur de charge distribue les flux d'information en calculant les meilleurs chemins réseaux afin d'accroître les performances et la disponibilité. Le groupe de servers qui reçoit le trafic peut être physiquement dispersé entre différents sites, permettant à l'application de continuer à fonctionner même s'il ne reste plus qu'un site opérationnel.

La figure n°18 ci-dessous illustre les avantages inhérents à la mise en cluster

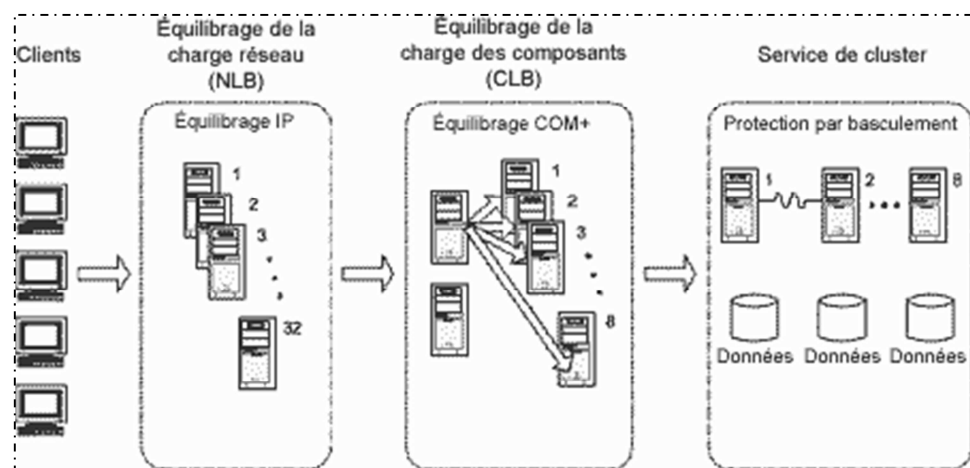


Figure n°18: Avantages de la mise en cluster

### 2.8.1.2. La réplication

La réplication permet de garantir la reprise de service sans nécessité de restaurer le système à partir de bandes de sauvegarde. On distingue deux types de répliquions:

- La réplication asynchrone: C'est une technique qui utilise la copie entre disques pour répliquer toute modification apportée au server nominal (server à protéger)

sur le server répliqué (server de secours). Les mises à jour du server répliqué ne se font pas en temps réel mais par lots.

- La réplication synchrone: Cette technique est analogue à la réplication asynchrone mais s'effectue en temps réel. Chaque modification opérée sur le server nominal étant répercutée instantanément sur le server répliqué.

### **2.8.1.3. La sauvegarde à distance**

La sauvegarde à distance consiste à réaliser des sauvegardes sur un support distant, généralement sur un site de secours pour permettre une réactivité plus grande en cas de sinistre. Cette technologie présente tous les avantages de la sauvegarde en ligne dont elle est un cas particulier).

### **2.8.1.4. La journalisation distante**

La journalisation distante s'effectue lorsque les changements apportés sur un server sont transmis automatiquement entre chaque sauvegarde classique sur un site distant, pour reconstituer, au fil de l'eau, un système au plus proche du système à secourir. Ces techniques nécessitent, par nature, un site distant de secours.

### **2.8.1.5. La virtualisation de stockage**

La virtualisation de stockage consiste en la « mise en commun logique d'éléments de stockage qui étaient indépendants à l'origine (différentes baies de stockage par exemple). Les principales technologies de virtualisation qui ont une utilisation en architecture de haute disponibilité sont les architectures de stockage en réseau (par opposition à l'attachement direct de type DAS) principalement représentées par les NAS et SAN.

## **2.8.2. Typologie**

La solution la plus répandue pour assurer le secours des données et applications critiques d'un système d'information est le site alternatif de secours, qui permet de bénéficier à l'optimum de la plupart des techniques ci-dessus présentées. Englobant divers types de solutions, allant des moins réactives (et les moins coûteuses) aux



solutions dites de haute disponibilité (les plus coûteuses). Une typologie des sites alternatifs est présentée ci-après:

- Salles blanches : Il s'agit d'une infrastructure distante de type salle informatique dédiée et disponible en cas de déclenchement du plan de secours. Cette salle est pré équipée pour accueillir les équipements informatiques, de telle sorte qu'en cas de déclenchement du plan de secours, l'entreprise vient littéralement «peupler» la salle blanche par les équipements informatiques.
- Salles orange: Il s'agit en général d'une salle blanche partiellement équipée de matériel informatique (les plus stratégiques). Il peut d'ailleurs s'agir d'un site de production informatique autonome, moins stratégique que le site à secourir, qui est aménagé pour servir de secours.
- Salles rouges : Une salle rouge est une salle blanche qui possède un environnement « peuplé latent », c'est-à-dire l'ensemble des équipements informatiques nécessaires au secours, maintenu en état de marche. Les données et applicatifs ne sont en revanche installés qu'en cas de déclenchement du plan de secours. En général, la salle rouge dispose d'un personnel permanent, dédié et prêt à mettre en place le secours.
- Salles miroir : Il s'agit de salles pleinement redondantes par rapport à la salle à secourir. Ainsi, en plus de l'équipement informatique complet, les données, systèmes et applicatifs y sont maintenus en permanence.

### 2.8.3. Topologies

Suivant la distance entre le site de production et le site de secours, différentes architectures et modes de réplication sont possibles:

- **Le « Campus Cluster »**

Dans ce type de cluster, les nœuds sont séparés dans deux (02) pièces différentes, voire deux (02) bâtiments, mais sur un même terrain privé. Il n'y a pas de contrainte pour passer les câbles et les distances sont courtes. La figure n°19 illustre l'architecture de cette topologie.

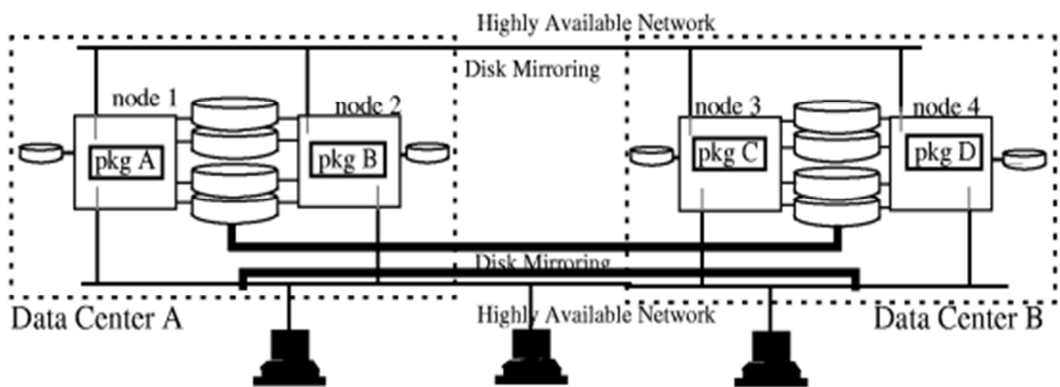


Figure n°19 : Architecture du « campus cluster »

- Le « Metropolitan cluster »

Dans ce type de cluster, ci-dessous illustré par la figure n°20, les nœuds sont hébergés par deux (02) bâtiments dans une même ville ou dans deux villes adjacentes. Ce type d'architecture assure une meilleure protection en cas de désastre, mais est plus complexe à mettre en œuvre car il faut relier les 2 bâtiments à travers une zone publique.

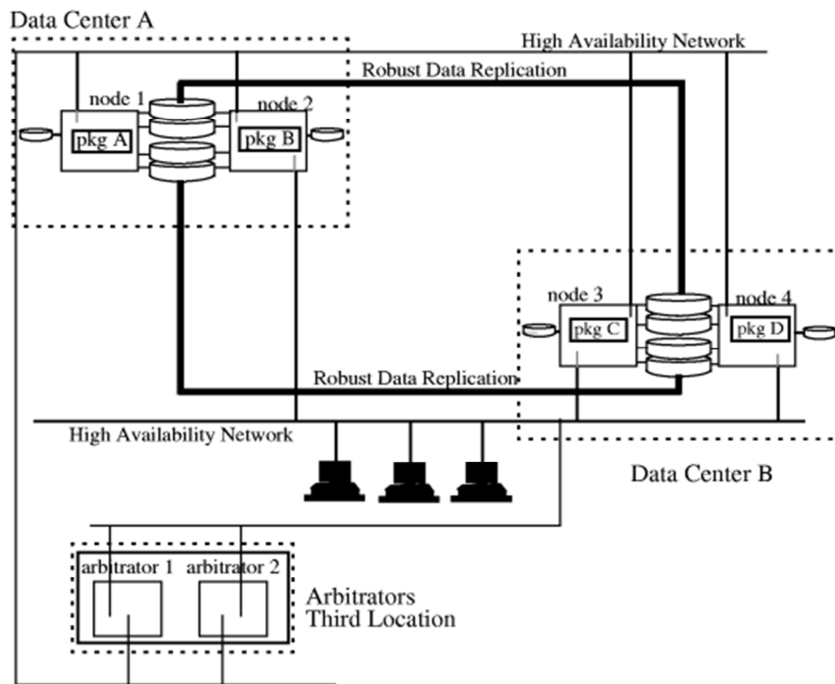


Figure n°20: Architecture du « Métropolitain Cluster »

- **Le « Continental cluster »**

Dans ce type de cluster, les nœuds sont séparés par une grande distance. La réplication s'appuie sur une liaison de type WAN en TCP/IP et s'effectue en mode asynchrone pour pallier aux temps de latence des liaisons WAN. La figure n°21 met en évidence l'architecture du « continental Cluster »

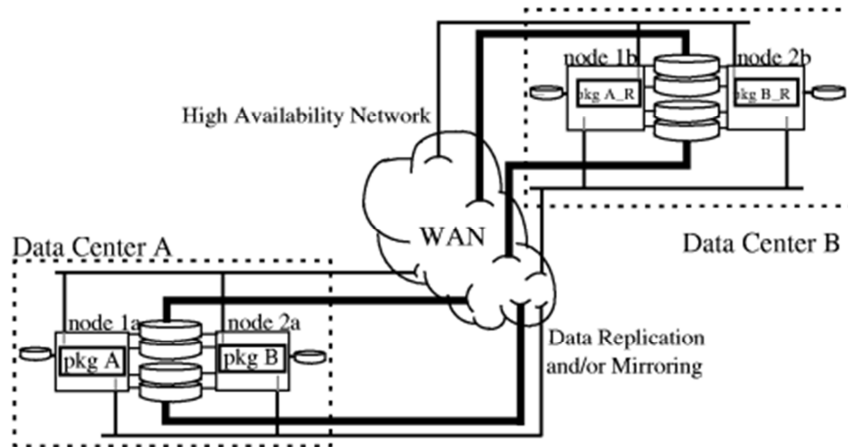


Figure n°21: Architecture du « Continental Cluster »

### **3. Réalisation pratique**

#### **3.1. Cadrage du projet DRP**

Suite à la décision de la direction générale d'OBSA de s'engager dans un processus visant à améliorer la résilience de son système d'information, une note de cadrage a été réalisée. Nous en présentons la teneur dans ce chapitre.

##### **3.1.1. Rappel du contexte**

Le projet DRP (Disaster Recovery plan) a été initié au sein de l'entreprise OBSA suite à la décision du groupe AOG de mettre en place un plan de continuité d'activité dans toutes ses filiales. Le référentiel PPM du groupe met en exergue les attentes du groupe en matière de continuité d'activité et l'implication attendue de la Direction générale dans le processus d'élaboration d'un PCA. Le projet DRP est coordonné au niveau du groupe, par le «DRP Group Administrator» en collaboration avec le RIT (Responsable Informatique et Télécoms) de la filiale qui en gère le volet opérationnel.

##### **3.1.2. Enjeux et objectifs**

La société OBSA de par son activité (Stockage et distribution de produits pétroliers) et son organisation est fortement dépendante des moyens informatiques. En effet, la plupart des activités sont gérées via un ERP (Enterprise resource planner) et la communication entre les acteurs de la chaîne de valeur dépend fondamentalement d'un logiciel de messagerie, d'une liaison VSAT et des autocommutateurs. Il va s'en dire, qu'une perte des moyens informatiques porterait un coup fatal au fonctionnement de l'entreprise. Ainsi donc, le projet DRP, en droite ligne avec les exigences du PPM a donc pour objectif global de:

- Protéger les processus métier cruciaux des effets causés par les défaillances du système d'information ou par des sinistres
- Réduire le risque d'interruption des affaires
- Garantir la reprise d'activité suite à une interruption ou à un désastre.

Il en résultera un système d'information avec une meilleure résilience, caractérisé par la mise en place d'un dispositif organisationnel et technique permettant la continuité de l'activité en cas de sinistre.

### 3.1.3. Périmètre du projet

L'outil principal de production chez OBSA est le système d'information et le projet DRP dans sa phase pilote, couvre essentiellement les ressources du système d'information; notamment : Les données - Les servers - Le réseau Local - Le réseau WAN - Les postes de travail - La téléphonie - L'accès internet - Les archives - Le personnel. Il importe toutefois, de préciser que le secours de ces moyens précités sera dimensionné au prorata des besoins de la cible fonctionnelle, qui sera définie à l'issue de l'analyse de risque.

### 3.1.4. Démarche

La mise en œuvre du projet DRP s'articulera autour des trois (03) phases successives suivantes:

- Phase n°1: Elaboration
- Phase n°2: Implémentation
- Phase n°3: Maintien en condition opérationnelle

Phase du projet DRP	Etapes	Objectif
Phase n°1 - Elaboration	Etape n°1: Cadrage et définition du projet	Identification des besoins de continuité
	Etape n°2: Cartographie des sinistres	
	Etape n°3: Analyse d'impact	
	Etape n°4: Analyse de risques	
	Etape n°5: Choix de la stratégie et des moyens de continuité	Définition des solutions pour assurer la continuité des métiers et des fonctions critiques
Phase n°2 - Implémentation	Etape n°6: Conception et mise en place de l'infrastructure optimisée	Elaborer et mettre en place l'architecture de continuité
	Etape n°7: Rédaction des procédures informatiques de continuité	Elaborer les procédures de continuité et de reprise technique et fonctionnelles
	Etape n°8: Mise en place de la cellule de crise	Organiser la communication
	Etape n°9: Formation des équipes	Former et tester
	Etape n°10: Test d'intégration du PCIT	
Phase n°3 - Maintien en condition opérationnelle	Etape n°11: Mise à jour des procédures	Maintenance du PCIT
	Etape n°12: Test du plan	

Tableau IV : Phases du projet DRP

Chacune de ces phases répond à un ou plusieurs objectifs et se décompose en étapes constituant les jalons du projet, tel que présenté dans le tableau IV (ci-dessus).

### **3.1.5. Organisation du projet**

Trois différents comités interviennent dans la phase active du projet. Il s'agit des comités de pilotage, opérationnels et de l'équipe projet qui sont présentés ci-dessous:

#### **3.1.5.1. Comité de pilotage**

La mission du comité de pilotage (COFIL) est de rendre les arbitrages, de prendre les décisions stratégiques et financières. Il est composé de:

- Monsieur Florent Fernandez, DSI
- Monsieur Daniel Nunez, DRP Groupe Administrator
- Monsieur Thierry Jaques, IT Technical Manager
- Jérôme Besème, Directeur Général de la filiale
- Moi-même en tant que Responsable informatique de la filiale

La fréquence des réunions du COFIL est alignée sur les jalons du projet et la tenue des comités est sous la responsabilité du DSI.

#### **3.1.5.2. Comité opérationnel**

La mission du comité opérationnel est de faire le suivi opérationnel du projet. Il est placé sous la direction du COFIL à qui il rapporte. Il est composé de:

- Monsieur Daniel Nunez, DRP Group Administrator
- Monsieur Thierry Jaques, IT Technical Manager
- Moi-même, en tant que Responsable du projet DRP de la filiale OBSA

#### **3.1.5.3. Equipe projet**

La mission de l'équipe projet est de réaliser les différents chantiers du projet. Elle est en charge de la réalisation de l'analyse de risque, l'analyse d'impact sur l'activité, de la définition des moyens de continuité informatique, de la conception de l'infrastructure optimisée, de la rédaction des procédures, des tests et exercices. Elle est essentiellement constituée des responsables d'activité et moi-même, Notons que Les

chefs de services sont essentiellement mis à contribution pour l'élaboration et la validation du BIA.

### **3.1.6. Livrables**

Les livrables sont rattachés aux différentes étapes du projet. Le tableau V, met en évidence les livrables du projet DRP. Il importe par ailleurs de noter qu'étant donné le contexte, j'ai été le principal référent par rapport à tous les livrables.

<b>Phase du Projet DRP</b>	<b>N° d'ordre</b>	<b>Etapes</b>	<b>Livrables</b>
<b>Elaboration du Projet DRP</b>	<b>1</b>	Cadrage et définition du projet	Note de cadrage
	<b>2</b>	Cartographie des sinistres	Scénarios de sinistres retenus
	<b>3</b>	Analyse d'impact	Matrice BIA
	<b>4</b>	Analyse de risques	Plan de réduction des risques par processus
	<b>5</b>	Choix de la stratégie et des moyens de continuité	Stratégie de continuité du SI
<b>Implémentation du PCIT</b>	<b>6</b>	Mise en place de l'infrastructure optimisée	Solution technique de continuité en opération
	<b>7</b>	Procédures informatiques de continuité	Rédaction des Procédures informatiques de continuité
	<b>8</b>	Mise en place de la cellule de crise	Support de communication
	<b>9</b>	Formation des équipes	Support de sensibilisation et de formation
	<b>10</b>	Test d'intégration du PCIT	Rapport de tests du PCIT
<b>Maintien en condition opérationnelle</b>	<b>11</b>	Mise à jour des procédures	PCA à jour
	<b>12</b>	Test du PCSI	Rapport de test du PCSI

Tableau V: Livrables



### 3.1.7. Gestion de la documentation

Un projet DRP par essence, génère une lourde documentation. Ci-dessous, la manière dont cette documentation sera gérée durant la phase active du projet.

#### 3.1.7.1. Référencement


Les documents (plan, procédures, schémas...) produits dans cadre du projet DRP seront référencés de manière en assuré une exploitation aisée. Ainsi donc, l'entête de chaque document, à l'image de l'interview BIA ci-dessous présenté à la figure n°22, met en exergue

- Le code du projet DRP
- Le code de l'étape à laquelle le document a été produit
- Le code du type de document
- Le numéro de la version
- Le libellé du document
- L'extension du document

BCM Programme - BIA-Interviews

---

**Business Impact Analysis**



---

BIA information and document controls

<b>BIA NUMBER</b>	TRA-130121	<b>DATE OF BIA</b>	
<b>VERSION</b>	V1.0	<b>DATE OF REVIEW</b>	
<b>FILE LOCATION</b>	d:\conseil\clients\addax&oryx group\dropbox\bcm\bia\bia - interviews.docx		

---

Details of staff involved in the BIA Process

TRI	NAME	ROLE	MAIL
DAN			
FLF			
PHD			
RAM			

---

Document Control

DATE	REVISION   AMENDEMENT DETAILS & REASON	AUTHOR	ESCALATE TO VERSION
20/11/12	FIRST DRAFT	RAM	V0.0

---

BIA Sign Off

<b>NAME AND TITLE OF THE OFFICER SIGNING OF THE BIA</b>	
<b>SIGNATURE :</b>	<b>DATE</b>

Addax & Oryx Group – BCM –
Confidential - 1 -

Figure N°22: Extrait de référencement

### **3.1.7.2. Stockage des documents**

Durant la phase active du projet, la documentation issue du projet sera sauvegardée sur un espace de stockage sécurisé et régulièrement sauvegardé. A cet effet, il a été créé sur le serveur de fichier « DWBJCOO1-415 » un dossier pour chaque étape du projet, lesquels dossiers contiennent chacun des sous dossiers couvrant les différents types de documents.

### **3.1.7.3. Circuit des documents**

Le comité de projet est producteur des documents, le comité d'opérationnel approuve les documents et le comité de pilotage valide les documents. Les approbations de documents se feront au cours des réunions du comité d'exploitation et les Validations aux cours des comités de pilotage.

### **3.1.8. Planning prévisionnel**

Il a été élaboré avec le logiciel « MS Project » un planning prévisionnel des différentes étapes du projet, précisant les étapes, les dates de début et de fin ainsi que les acteurs. Le tableau VI ci-dessous, présente un aperçu de ce planning.

Task Name	Duration	Start	Finish	Predecessors	Resource Name
Projet DRP Oryx Benin SA Filiale du Groupe AOG	160 days?	Mon 30/07/12	Fri 08/03/13		
Elaboration du Projet DRP	95 days?	Mon 30/07/12	Fri 07/12/12		F. Yelouassi [70%];D. Nunez [20%];F. Fernandez [10%]
Cadrage et définition du projet	5 days	Mon 30/07/12	Fri 03/08/12		
Cartographie des sinistres	17 days	Mon 06/08/12	Tue 28/08/12		F. Yelouassi [80%];D. Nunez [20%]
Identification des menaces potentielles	5 days	Mon 06/08/12	Fri 10/08/12		
Evaluation des probabilités et impacts	10 days	Mon 13/08/12	Fri 24/08/12	5	
Identification des menaces caractérisées	2 days	Mon 27/08/12	Tue 28/08/12	6	
Analyse d'impact	59 days	Mon 30/07/12	Thu 18/10/12		F. Yelouassi [80%];D. Nunez [20%]
Identification des activités	9 days	Wed 29/08/12	Mon 10/09/12		
Estimation des impacts financiers et opérationnels	5 days	Tue 11/09/12	Mon 17/09/12		
Détermination des processus critiques	3 days	Tue 18/09/12	Thu 20/09/12	14;15	
Détermination des configurations	49 days	Mon 30/07/12	Thu 04/10/12		
Détermination des paramètres de reprise	10 days	Fri 05/10/12	Thu 18/10/12		
Rédaction des procédures de secours	8 days	Mon 30/07/12	Wed 08/08/12		
Analyse de risques	18 days	Fri 21/09/12	Tue 16/10/12		F. Yelouassi [80%];D. Nunez [20%]
Cartographie des risques	8 days	Fri 21/09/12	Tue 02/10/12		
Elaboration du plan de réduction des risques	10 days	Wed 03/10/12	Tue 16/10/12	30	
Elaboration de la stratégie de continuité					
Expression des besoins en termes de continuité	8 days	Wed 17/10/12	Fri 26/10/12		
Elaboration des moyens techniques de continuité	55 days	Thu 02/08/12	Wed 17/10/12		
Etude de faisabilité	5 days	Mon 03/12/12	Fri 07/12/12	41;39;40	
Implémentation	50 days	Mon 10/12/12	Fri 15/02/13		F. Yelouassi [60%];T. Jaques [10%];D. Nunez [20%];F. Fernandez [10%]
Mise en place de l'infrastructure optimisée	10 days	Mon 10/12/12	Fri 21/12/12	42	
Rédaction des procédures informatiques de continuité	20 days	Mon 24/12/12	Fri 18/01/13	44	
Mise en place de la cellule de crise	5 days	Mon 21/01/13	Fri 25/01/13	45	
Formation des équipes	10 days	Mon 28/01/13	Fri 08/02/13	46	
Tests d'intégration du PCIT	5 days	Mon 11/02/13	Fri 15/02/13	47	
Maintien en condition opérationnelle	15 days	Mon 18/02/13	Fri 08/03/13		F. Yelouassi. Nunez; F. Fernandez; T. Jaques. Aguessy; Kindji; Hounsou; Tossou
Mise à jour des plans	10 days	Mon 18/02/13	Fri 01/03/13	48	

Tableau VI: Extrait du Planning Projet DRP

## **3.2. Cartographie du Système d'information**

Cette étape du projet a été caractérisée par la collecte des éléments nécessaires à l'analyse, en réalisant un découpage du système d'information par rapport aux processus métiers supportés, pour ainsi aboutir à un relevé des actifs par processus.

### **3.2.1. Découpage du SI**

Il a été réalisé un découpage du SI d'OBSA, associant à chaque sous système, les fonctions supportées et à chaque fonction, les processus métier gérés.

#### **3.2.1.1. Le système d'information opérationnel**

Le rôle du SI opérationnel est de collecter, mémoriser, traiter les données nécessaires à la conduite de l'activité, ainsi que d'automatiser, fluidifier et optimiser les processus, le SI opérationnel d'OBSA supporte les activités suivantes:

- **Opérateurs**

La fonction « opérateur » a pour objectif de gérer la réception et le transfert en bac des produits pétrolier (hydrocarbures, gaz, lubrifiant), livrés par des navires marchands, le chargement et l'expédition de produits pétroliers.

- **Administration des ventes**

La fonction « ADV » consiste à gérer la réception des commandes clients, l'élaboration des commandes, la gestion de la logistique et assurer le reporting des ventes.

- **Comptabilité Client**

La comptabilité Client a pour objectif d'assurer la facturation des commandes clients ; gérer la situation client (limite de crédit, délai de paiement...etc.) ; Assurer le reporting de la comptabilité client.

- **Comptabilité fournisseur**

La comptabilité fournisseur gère le traitement des factures fournisseur; la situation fournisseur; le reporting de la comptabilité fournisseur

- Comptabilité matière:

La comptabilité matière gère les stocks de produits pétroliers (HC, LUB, GPL), produit et communique les états de stocks ainsi que le « stock report » suivant une contrainte temporelle.

- Comptabilité Générale

La fonction « Comptabilité Générale » Gère l'élaboration du budget, les immobilisations, le paramétrage des comptes et la fiscalité.

- Gestion des ressources humaines

La fonction GRH consiste à gérer la paie et les ressources humaines de l'entreprise.

### **3.2.1.2. Le système d'information d'aide à la décision**

Le rôle du système d'information d'aide à la décision est de fournir des indicateurs pertinents sur l'activité ainsi que des outils d'analyse et de simulation. Le SI d'aide à la décision d'OBSA supporte les activités suivantes

- Contrôle de gestion

La fonction « contrôle de gestion » Gère les KPI ; contrôle les reporting des différents services; Gère le « Capex report ».

- Reporting et consolidation

La fonction « reporting et consolidation » Gère la consolidation et l'élaboration du reporting comptable suivant une contrainte temporelle.

### **3.2.1.3. Système d'information de communication**

Le rôle du SI de communication est de soutenir la communication des informations en interne et les échanges avec les partenaires (clients et fournisseurs). Le SI de communication chez OBSA supporte fondamentalement la partie de la fonction informatique qui consiste à gérer la messagerie et administrer le réseau informatique et de télécommunication.

Le découpage du SI a permis d'établir un récapitulatif des processus métier en associant à chaque processus un responsable, le logiciel utilisé, le nombre et le type exact de matériel IT utilisé pour l'exécution du processus. La figure n°23 met en évidence le découpage du SI d'OBSA qui servira de base à l'élaboration d'une cartographie complète des processus avec le logiciel spécialisé « ADONIS ».

Système d'information	Fonction supportée	Processus métier	Responsable du processus	Matériel IT utilisé			Accès internet
				Logiciel	Autre matériel	Quantité	
SI Opérationnel	Opérateur	Confirmer chargement	Chefs d'équipe	JDE	PC Client	4	NON
		Elaborer point de chargement		Suite Micosoft office	Imprimante matricielle	2	
		Libérer camion			JDE	Imprimante laserjet	
	Administration des ventes	Gérer commande client	Tatiana Toviakou	JDE	Poste téléphonique	4	OUI
					Interphone accès restreint	1	
		Téléphone ligne directe		1			
		Gérer logistique		Excel	Imprimante laserjet	1	
	Elaborer Point des commandes	Olivier Hodonou	Suite Micosoft office	PC Client	1	1	
				Imprimante deskjet	1		
	Interphone accès restreint					1	
	Comptabilité client	Gérer facturation client	Arius Agbagan	JDE	PC Client	1	OUI
					Imprimante laserjet	1	
		Elaborer Reporting compta client		Suite Micosoft office	Interphone accès restreint	1	
					Mettre à jour fichier client	Clotilde	
	Libérer commande		JDE	Interphone accès restreint	1		
	Comptabilité Fournisseur	Gérer facture fournisseur	Ygnace Tossou	JDE	Poste Client	1	OUI
					Interphone accès restreint	1	
		Elaborer reporting compta fournisseur		Suite Micosoft office	Téléphone ligne directe	1	
	Gérer situation fournisseur		JDE				
	Comptabilité Matière	Gérer stock	Barthélémy Zinsou	JDE	Poste Client	1	NON
				Vigilens	Interphone accès restreint	1	
				Suite Micosoft office	Imprimante laserjet	1	
	Comptabilité Générale	Elaborer budget	Pierre Biton	Suite Micosoft office	Adobe		OUI
PC client					1		
Imprimante laserjet		1					
Gérer immobilisation		Charles Kindji	JDE	Interphone accès libre	1		
				01 PC client	1		
Interphone accès restreint		1					
Paramétrer comptes			Suite Micosoft office	Interphone accès restrict	1		
	JDE			1			
Gérer fiscalité	Rodrigue Boccovo	JDE	PC Client	1			
GRH	Gérer Paie	Aimée Gouyidji	Sage Saari	Interphone accès restreint	1	OUI	
				Interphone accès libre	1		
	Gérer temps de travail			Scaneur	1		
				Imprimante deskjet	1		
	Gérer ressources externes	Charlemagne Durand	Sage Saari	PC Client	1		
Gérer carrière		Sage Saari	Interphone accès libre	1			
SI d'aide à la décision	Contrôle de gestion	Romuald Adjivon	Suite Micosoft office	Imprimante deskjet	1	OUI	
				Interphone accès libre	1		
	Reporting et consolidation	Sostène Hounsou	HFM	PC Client	1	OUI	
			JDE				
Elaborer reporting		Exel	Interphone accès libre	1			
SI d'aide à la communication	Informatique	Gérer support de communication	Francis Yelouassi	Exécutables - Licence - Documentation de tous les logiciels	PC Client	4	OUI
					Serveur physiques DL 385	4	
					Routeur	3	
					Liaison BLR		
Liaison VSAT	1						

Figure n°23: Découpage du SI d'OBSA

### 3.2.2. Architecture réseau

OBSA a adopté la technologie Ethernet (10/100/1000) avec le protocole IP comme fédérateur du réseau informatique. Les serveurs d'AD, DNS et DHCP sont installés sur des serveurs Windows 2003 Enterprise Edition. Le réseau informatique d'OBSA est constitué de trois sites principaux interconnectés et deux sites isolés. On distingue:

- Le site de la direction générale situé à Cotonou dans la zone commerciale de « Ganhi » qui abrite l'infrastructure IT principale et le service informatique. Ce site est constitué des actifs suivants:
  - 03 Servers physiques HP DL 385 émulant 05 serveurs virtuels
  - 01 lecteur de tape LTO 4
  - 40 PC client
  - 04 switch Cisco
  - 01 routeur CISCO
  - 01 autocommutateur Hipath 3800
  - 10 imprimantes
  - 01 modem Redline AN – 30<sup>e</sup> Terminal (Antenne Radio)
  - 01 modem Comtech CDM – 570 (Antenne Satellite)
  - 01 antenne VSAT SUI – 29H3
  - 42 postes téléphoniques Siemens Optiset E Standard
  - 01 riverbed
  
- Le site du dépôt hydrocarbure situé dans l'enceinte portuaire est à six (06) km environ du site de la direction générale. Le site du dépôt HC est relié au site de la direction générale via une liaison BLR de 2Mbds. Ce site est constitué des actifs suivants:
  - 01 Server physique HP ML 370
  - 01 server d'applications + fichiers
  - 01 lecteur de tape
  - 20 PC client
  - 03 Switch Cisco
  - 01 routeur CISCO 2800 série
  - 01 autocommutateur Hipath 3500
  - 09 imprimantes
  - 01 modem Redline AN – 30<sup>e</sup> Terminal (Antenne Radio)
  - 15 postes téléphoniques Siemens Optiset E Standard
  - 01 platine de brassage de la fibre optique
  - 01 riverbed SH250



- Le site du dépôt GPL, situé à 02 km du site du dépôt HC et interconnecté à ce dernier via une liaison fibre optique. Ce site contient les actifs suivants:
  - 01 routeur Cisco 2800 serie
  - 02 switches Netgear (GS 724 TP et GSM 7224)
  - 04 imprimantes
  - 15 téléphones IP–Siemens Open stage
  - Platine de brassage fibre optique
  
- Le site du service transit, situé dans l’enceinte du dépôt HC est interconnecté au réseau de la douane pour exploitation du logiciel Sydonia ++ de la douane Béninoise via une liaison BLR. Ce site est constitué de:
  - 01 routeur
  - 01 Switch
  - 6 PC
  - 03 imprimantes matricielles pour l’impression des déclarations douanières
  
- Le site de la maison du gaz situé à 30 km du siège n’est pas interconnecté aux autres sites. Les échanges d’informations avec les autres sites se font via internet et des navettes en fin de journée. Ce site est constitué de deux PC – Une imprimante – une liaison ADSL.
  
- Le site du dépôt Lubrifiant basé à 10 km du siège n’est pas connecté au réseau informatique d’OBSA. Ce site est constitué d’un PC d’une imprimante et d’une connexion internet via une clé Edge.

Il importe de préciser que le réseau IT d’OBSA est interconnecté au réseau du Groupe AOG via une liaison VSAT mutualisée depuis 2009 et permettant de rendre variable les performances, notamment en terme de bande passante pour l’accès à internet et une intégration Voix et données à travers un réseau privé.

Les figures n°24 et n°25 illustrent respectivement l’architecture réseau détaillé d’OBSA et la position du réseau d’OBSA au sein de la forêt AOG.

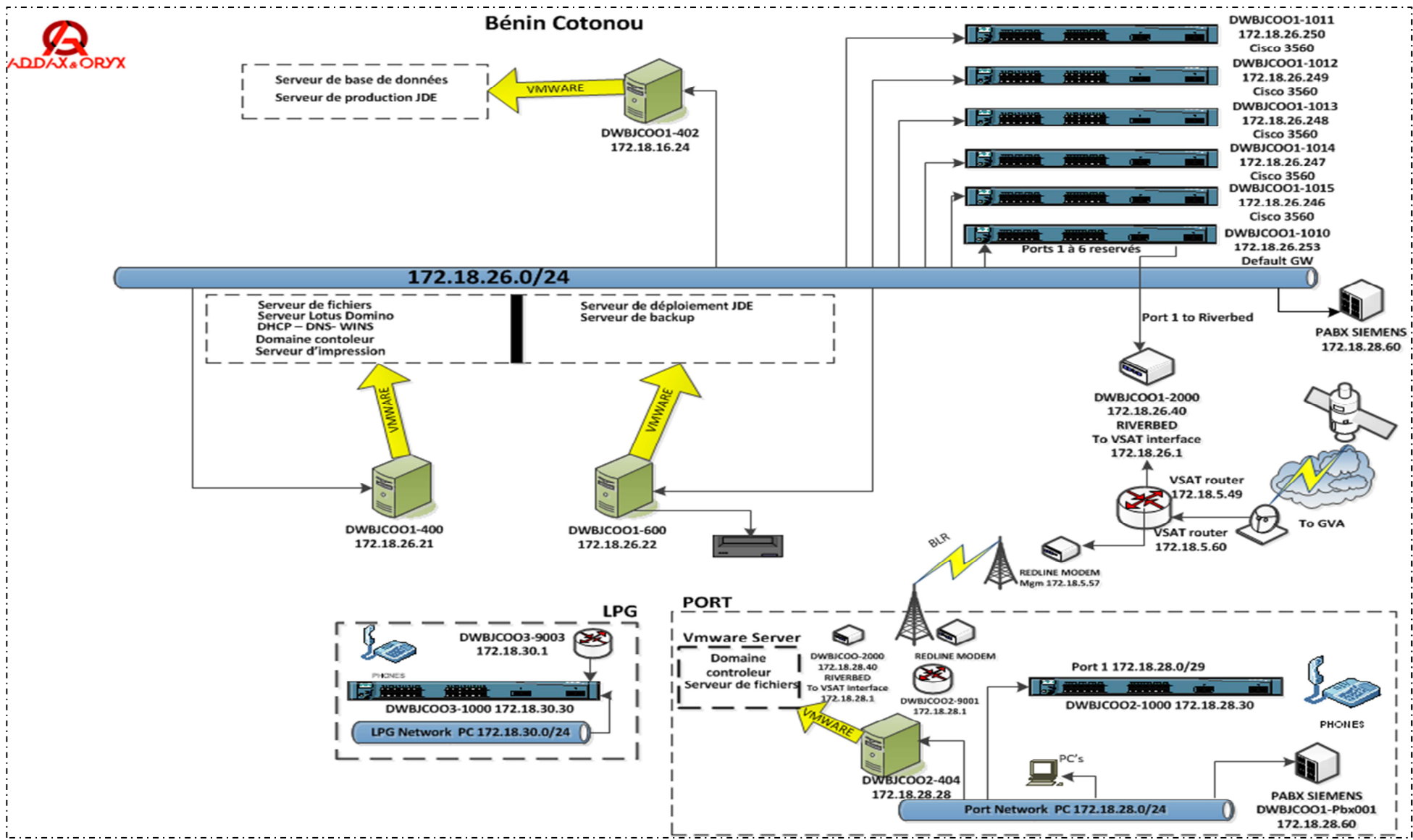


Figure n°24: Topologie réseau d'OBSA

# AOG Communication Network Synopsis (with Riverbed)

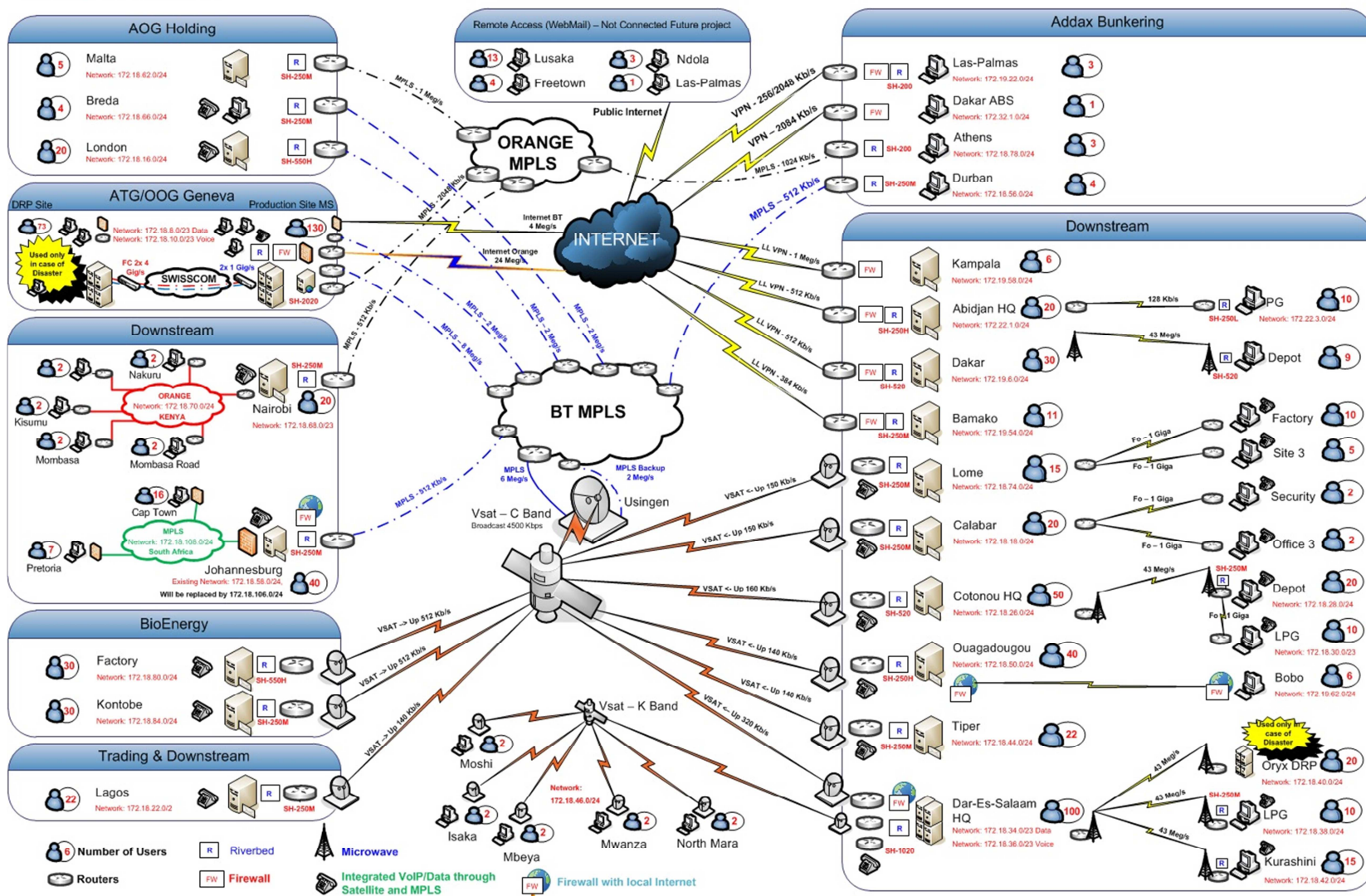


Figure n°25: Topologie « Forêt AOG »

### 3.2.3. L'accès à internet

OBSA dispose de deux différents points d'accès à internet:

- Une liaison VSAT d'une bande passante variable puisque mutualisée avec les autres sites de la société.
- Une liaison ADSL dédiée à la maintenance distante des équipements VSAT.

### 3.2.4. Les autocommutateurs

Les autocommutateurs de la direction et du dépôt sont gérés suivant une politique de restriction, limitant suivant les besoins des utilisateurs, l'accès à l'international via satellite, aux appels locaux (à l'intérieur du Bénin), ou uniquement aux numéros. Il est également appliqué une politique d'interception par groupe de proximité. Cette politique a été validée par la Direction générale et fait office d'un audit annuel.

La figure N° 26 présente un extrait de la configuration IP des autocomms au dépôt GPL d'OBSA.

Pabx Modèle :	<b>Siemens HIPATH 3500</b>				
Host Name (FQN) :	<b>DWBJCOO2-PBX02</b>				
Configuration IP (Management LIMS) :	<b>172.18.28.60</b>	Subnet	<b>255.255.255.0</b>	Gateway:	<b>172.18.28.1</b>
Configuration IP (Gateway) :	<b>172.18.28.62</b>	Subnet	<b>255.255.255.0</b>	Gateway:	<b>172.18.28.1</b>
Plan de numérotation interne :	<b>4200 à 4399</b>				<b>--&gt; 200 Numeros attribués</b>
Numéros principales analogiques :		tbd			<b>--&gt; 2 Lignes</b>
		tbd			

Figure N°26: Vue partielle configuration autocommutateur

### 3.2.5. Les Logiciels

Plusieurs logiciels sont utilisés chez OBSA. Tous ces logiciels ont été acquis légalement et possèdent un numéro de licence officielle. Un fichier de gestion des licences de logiciel a été mise en place et audité chaque année. Les logiciels communs font office d'une commande globale, en vue de limiter les coûts. Ci-dessous (tableau VII), un inventaire des principaux logiciels en vogue chez OBSA.

<b>Logiciel</b>	<b>Utilisation</b>	<b>Interface</b>	<b>Base de données</b>
<b>JDE</b>	Gestion des opérations Gestion des de la comptabilité Client Gestion de la comptabilité fournisseur Gestion de la comptabilité Générale Gestion des immobilisations Gestion stocks	<a href="#">Full web</a>	SQL Server
<b>Sage Saari</b>	Gestion de la paie Gestion des ressources humaines	NA	Propriétaire
<b>Vigilens</b>	Elaboration d'états financiers et de gestion	NA	SQL Server
<b>Etatsoft</b>	Comptabilité avant JDE	NA	SQL Server
<b>HFM</b>	Consolidation	<a href="#">Full web</a>	NA
<b>Suite MS Office</b>	Traitement de texte Tableur SGBD	NA	NA

Tableau VII: Extrait de l'inventaire Logiciel d'OBSA

### 3.3. Cartographie des sinistres

OBSA ne disposant pas d'une grille standard d'évaluation des risques, indispensable à la cartographie des sinistres, j'en ai réalisé une, inspirée des différentes grilles de statut fournies par la méthode MEHARI. Basée sur des éléments de jugement permettant d'évaluer la sévérité de chaque scénario de sinistre, les métriques ont été établies en collaboration avec les responsables métiers et ont fait l'objet d'une validation par le comité de pilotage du projet DRP. La grille ainsi obtenue permettra également, de fixer les objectifs de continuité en fonction de niveaux préétablis d'acceptation ou de refus total des risques encourus.

#### 3.3.1. Grille d'évaluation

Je présente à cette étape, les différents paramètres et le processus ayant conduit à l'élaboration d'une grille standard d'évaluation des sinistres pour OBSA.

##### 3.3.1.1. Métriques des mesures de protection

Il s'est agi à cette étape, de mesurer l'effet des mesures de protection existante, en cas d'avènement d'un sinistre. Le tableau VIII présente le statut des mesures de protection adopté chez OBSA en fonction du niveau de protection offert face au sinistre.

STATUT	EFFET DES MESURES DE MESURES DE PROTECTION SUR L'IMPACT
1	Effet de protection très faible: le sinistre ne sera détecté qu'au bout d'un délai important. Les mesures qui pourront alors être prises ne pourront limiter la propagation de l'incident initial et se limiteront à la borner dans le temps. L'étendue des conséquences du sinistre est difficile à cerner.
2	Effet de protection moyen: le début de sinistre ne sera pas identifié très vite et les mesures prises le seront tardivement. Le sinistre aura pris une grande ampleur mais l'étendue de ses conséquences sera encore identifiable.
3	Effet important: le sinistre sera détecté rapidement et des mesures de protection seront prises sans délai. Le sinistre aura néanmoins eu le temps de se propager, mais les dégâts seront circonscrits et facilement identifiables.
4	Effet très important: le début de sinistre sera détecté en temps réel et les mesures déclenchées immédiatement. Le sinistre sera limité aux détériorations directes provoquées par l'accident, l'erreur ou la malveillance.

Tableau VIII : Statut des mesures de protection (Source CLUSIF)

### 3.3.1.2. Métrique des mesures palliatives

Les mesures palliatives sont les dispositions prises en vue d'assurer la continuité de l'activité en cas d'avènement du sinistre. Le tableau VIV présente le statut des mesures palliatives retenu par le comité opérationnel et validé par le comité de pilotage

STATUT	EFFET DES MESURES PALIATIVES SUR L'IMPACT DU SCENARIO
1	Effet très faible: les solutions de secours éventuellement nécessaires doivent être improvisées. Il n'est pas assuré que les activités de l'entreprise touchées par le sinistre pourront être poursuivies. L'activité de l'ensemble des acteurs touchés par le sinistre est très fortement perturbée.
2	Effet moyen: les solutions de secours ont été prévues globalement et pour l'essentiel, mais l'organisation de détail reste à faire. Les activités principales touchées pourront se poursuivre après un temps d'adaptation qui peut être long. La reprise des autres activités et le retour à l'état d'origine demandera des efforts importants et occasionnera une forte perturbation des équipes.
3	Effet important: les solutions de secours ont été prévues, organisées dans le détail et validées. Les activités principales pourront se poursuivre après un temps de reconfiguration acceptable et connu. La reprise des autres activités et le retour à l'état d'origine ont également été prévus et se dérouleront avec des efforts importants mais supportables.
4	Effet très important: le fonctionnement des activités de l'entreprise est assuré sans discontinuité notable. La reprise de l'activité en mode normal est planifiée et sera assurée sans perturbation notable.

Tableau VIV: Statut des mesures palliatives d'OBSA

### 3.3.1.3. Métrique des mesures de récupération

Cette rubrique des métriques comme présentée dans le tableau X, servira à évaluer le niveau de couverture en termes d'assurance de l'entreprise.

STATUT	EFFET DES MESURES DE RECUPERATION SUR L'IMPACT
1	Effet très faible: ce que l'on peut espérer récupérer des assurances ou d'un recours en justice est négligeable devant l'ampleur des dégâts subis.
2	Effet moyen: ce que l'on peut raisonnablement espérer récupérer n'est pas négligeable, mais les sinistres majeurs restent à la charge de l'entreprise (sinistre non couvert et responsable non solvable).
3	Effet important: l'entreprise est couverte pour les sinistres majeurs, mais ce qui reste à sa charge (franchise) demeure important quoique supportable.
4	Effet très important: l'entreprise est suffisamment couverte pour que l'impact financier résiduel soit négligeable.

Tableau X: Statut des mesures de récupération

### 3.3.1.4. Métrique des mesures réduction du risque

Ces métriques tels que présentés sur le tableau XI permet d'évaluer, l'impact des mesures de réduction, en cas d'avènement d'un sinistre.

STATUT	EFFET DES MESURE PRISE SUR LA REDUCTION D'IMPACT DES SCENARIOS
1	Effet très faible
2	Effet moyen : impact maximum jamais supérieur à un impact grave : $I \leq 3$
3	Effet important : impact maximum jamais supérieur à un impact moyennement grave : $I \geq 2$
4	Effet très important : impact du scénario toujours négligeable quel que soit l'impact intrinsèque

Tableau XI: Statut des mesures de réduction du risque

### 3.3.1.5. Exposition naturelle

L'évaluation du statut d'exposition naturelle au sinistre a pour objectif d'estimer les failles ou avantages naturelles liées à l'environnement de l'entreprise face à un scénario de sinistre. Le tableau XII met en évidence ces métriques telles qu'adoptée par OBSA.

STATUT	EFFET DES MESURES STRUCTURELLES SUR LA POTENTIALITE
1	Exposition très faible: Des mesures architecturales ont été prises pour limiter structurellement les risques (cloisonnement des locaux, fragmentation des informations, rendant négligeable la probabilité d'un risque majeur).
2	Exposition faible: L'entreprise est particulièrement peu exposée; le climat social est très favorable, l'environnement ne laisse pas craindre le moindre problème, la position de suiveur de l'entreprise rend peu probable une agressivité notable de concurrents.
3	Exposition moyenne: L'entreprise n'est pas particulièrement exposée. Le climat social n'est pas mauvais, la concurrence est normalement agressive sans plus, l'environnement ne présente pas de menace particulière.
4	Exposition importante: L'entreprise est particulièrement exposée au risque envisagé de par un climat social très défavorable ou un environnement à risque ou une position telle que l'on peut craindre des réactions spécialement agressives de la concurrence.

Tableau XII: Statut d'exposition au risque



### 3.3.1.6. Mesures dissuasives

Les mesures dissuasives sont constituées des dispositions adoptées par l'entreprise pour décourager toute démarche néfaste à l'entreprise. Il importe dans ce cas de communiquer par rapport à ce point et exposer clairement les sanctions en cas d'avènement. Ces mesures contribuent à limiter la probabilité d'avènement d'une certaine catégorie de sinistre et les métriques exposées dans le tableau XIII, les présentes telles qu'adoptés par OBSA.

STATUT	EFFET DES MESURES DISSUASIVES SUR LA POTENTIALITE
1	Effet très faible: L'auteur n'encourrait aucun risque; il n'a pratiquement aucun risque d'être identifié et de toute façon cela n'aurait pour lui aucune conséquence.
2	Effet moyen: L'auteur encourrait un risque faible; le risque d'être identifié est faible et les sanctions éventuelles, s'il était découvert, resteraient supportables.
3	Effet important: L'auteur de l'erreur ou de la malveillance encourrait un risque important; il existe une forte probabilité qu'il soit découvert et les sanctions encourues pourraient être graves.
4	Effet très important: Seul un inconscient pourrait courir un tel risque; il sera démasqué à coup sûr, les sanctions seront très lourdes et tout cela est bien connu.

Tableaux XIII: Statut des mesures dissuasives chez OBSA

### 3.3.1.7. Mesures préventives

Il s'agit ici des dispositions prises pour repousser au maximum l'avènement d'un sinistre donné. L'évaluation de ces mesures dans le contexte d'OBSA tel que retenu se présente ci-dessous (tableau XIV).

STATUT	EFFET DES MESURES PREVENTIVES SUR LA POTENTIALITE
1	Effet très faible: Toute personne de l'entreprise ou tout initié la connaissant un minimum est capable de déclencher un tel scénario, avec des moyens qu'il est facile d'acquérir. Des circonstances tout à fait courantes (maladresse, erreur, conditions météo défavorables rares mais n'ayant rien d'exceptionnel) sont à même de déclencher un tel scénario.
2	Effet moyen: Le scénario peut être mis en œuvre par un professionnel sans autres moyens que ceux dont font usage les personnels de la profession. Des circonstances naturelles rares mais non exceptionnelles peuvent aboutir à ce résultat.

3	Effet important : Seul un spécialiste ou une personne dotée de moyens importants décidée à y consacrer du temps peut aboutir dans la réalisation d'un tel scénario. Des concours de circonstances peuvent rendre le scénario plausible.
4	Effet très important: Seuls quelques experts sont capables, avec des moyens très importants, de mettre en œuvre un tel scénario. Au niveau des événements naturels, seules des circonstances exceptionnelles peuvent conduire à de tels résultats (catastrophes naturelles).

Tableau XIV: Statut des mesures préventives chez OBSA

### 3.3.1.8. Evaluation de l'impact

L'évaluation de l'impact réel du sinistre se fera en fonction du statut de réduction du risque et du degré de criticité de la ressource; ce dernier s'obtiendra par une classification des ressources. Le niveau d'impact est issu du croisement des deux paramètres, tel qu'illustré par la matrice de la grille de la figure n°27.

Classification de la ressource STATUT -RI	1	2	3	4
	1	1	2	3
2	1	2	3	3
3	1	2	2	2
4	1	1	1	1

Figure n°27 : Grille d'évaluation de l'impact du risque chez OBSA

### 3.3.1.9. Potentialité

La grille d'évaluation du statut de probabilité d'avènement d'un sinistre est essentielle dans une démarche d'analyse de risque. L'entreprise s'en inspire pour définir sa stratégie de gestion de risque. Le tableau XV, met en évidence la grille d'évaluation de la probabilité d'avènement des risques chez OBSA.

STATUT	POTENTIALITE
1	Potentialité faible, ne surviendra sans doute jamais
2	Possible, bien que potentialité faible
3	Potentialité certaine, devrait arriver un jour
4	Très forte potentialité, surviendra sûrement à court terme

Tableau XV: Grille d'évaluation du statut de potentialité






La méthode MEHARI propose une grille d'aversion au risque, construite sur la base de l'appréciation du risque, par rapport à son impact et à sa probabilité. S'y basant, le comité opérationnel du projet DRP a proposé la grille de la figure n°28, qui a été validé par le comité de pilotage. Rappelons que l'objectif in fine de cette grille est d'estimer la sévérité du risque en cas d'avènement, afin de définir dans le cadre d'une analyse de risque les mesures à adopter pour ramener cette sévérité à un niveau acceptable, dans un contexte où l'entreprise ne disposerait pas des moyen nécessaires pour supporter l'impact en cas d'avènement du risque ou souhaiterait tout court, s'en protéger.

	P	0	1	2	3	4
I						
4	● 0	● 0	● 3	● 4	● 4	● 4
3	● 0	● 0	● 2	● 3	● 3	● 3
2	● 0	● 0	● 1	● 2	● 2	● 3
1	● 0	● 0	● 0	● 0	● 1	● 1

Figure n°28: Grille d'évaluation de la sévérité du risque

La règle adoptée pour l'exploitation de cette grille est la suivante:

**P** : Probabilité; **I** : Impact

 0	→ Risque insignifiant	 1	→ Risque accepté
 3	→ Risque inadmissible	 4	→ Risque insupportable
 2	→ Risque toléré		

La grille d'évaluation des sinistres étant élaborée, le processus d'identification des menaces caractérisés a suivi normalement sont cours avec comme objectif de filtrer la liste générique des menaces fournies par le siège via le processus d'évaluation de la sévérité de ces menaces en cas d'avènement. La démarche adoptée a été de procéder directement à l'évaluation des probabilités et impact nets; c'est-à-dire, tenant comptes des dispositions de prévention et de protection existantes. Les résultats finaux ont été ensuite présentés au comité de pilotage.

### 3.3.2. Identification des menaces potentielles

Les principales menaces faces auxquelles le groupe AOG souhaite se prémunir sont présentées dans le tableau XVI. Cette liste de menaces a été soumise à toutes les filiales qui devront s’y baser pour effectuer leur analyse de risque. C’est une liste totalement flexible adaptable aux filiales, en fonction d’éléments pertinents comme par exemple la météorologie ou la sismologie de l’emplacement géographique de la filiale, qui sont évaluées à partir de la grille d’évaluation des impacts des sinistres.

Menaces
Tremblement de terre
Inondations
Feu
Explosions
Terrorisme
Produits Chimiques
Fumée
Grèves
Evènement Météorologique graves
Epidémies
Inondation Internes
Vol/Brigandage
Sabotage
Coupures de Courant
Coupures Internet
Coupures Téléphoniques
Négligences

Tableau XVI: Liste des menaces potentielles

### 3.3.3. Evaluation des probabilités

Je présente à cette étape, le processus ayant mené à l’affectation d’une probabilité d’avènement aux menaces potentielles.

#### 3.3.3.1. Hypothèses de départ

Une hypothèse de base de l’étude ayant menée à l’évaluation de la sévérité des scénarios de menace a été de considérer uniquement les sites de la Direction générale et du dépôt. Une seconde hypothèse a été de considérer les mesures palliatives, de protection, de récupération comme étant des dispositions de protection parce qu’intervenant en amont de l’avènement du risque pour en diminuer l’impact et les

mesures dissuasives et préventives comme étant des dispositions de prévention en ce sens qu'ils interviennent en aval du risque pour en diminuer la probabilité d'avènement.

### 3.3.3.2. Evaluation de la Potentialité

La potentialité est la probabilité qu'une menace survienne et dépend des dispositions de prévention mises en place. Il est clair que plus le dispositif de prévention est corsé, plus la probabilité que le danger survienne est faible. Afin de profiter de l'existant en termes de prévention, il a été mené une évaluation des mesures de prévention face aux menaces en question. Chaque menace a fait l'objet d'une analyse détaillée pour en évaluer le dispositif de prévention existant, afin d'aboutir à une estimation du statut de prévention sur une échelle de [1,4].

Dans le cadre de ce mémoire, je mets en exergue, les différents axes d'analyses ayant meublés les «brainstormings» qui ont conduit à l'évaluation des statuts de potentialité.

- **Tremblement de terre**

Les sites de l'entreprise sont situés dans une zone à faible activité sismique. Les archives de l'IGN (institut géographique nationale) révèlent zéro (0) tremblement de terre sur les cents dernières années et la carte de la figure n°29, étudiée dans ce cadre montre bien que le Bénin se situe dans une zone non sismique. Le statut de probabilité affecté à la menace « tremblement de terre » est de un (01)

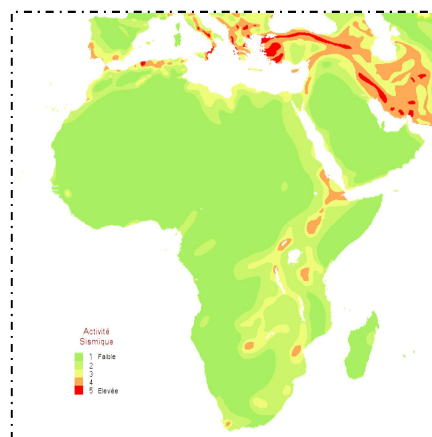


Figure n°29: Carte des zones sismiques

- **Inondations**

Le site de la direction d'exploitation étant situé au bord de la mer (figure n°30) et dans une zone où sévit une lutte permanent contre l'avancé de l'océan Atlantique, la probabilité qu'un jour, sévisse l'inondation est certaine. Le statut de probabilité affecté à cette menace est de niveau trois (03).



Figure n°30: Aperçu Google Earth du terminal OBSA

- **Feu**

Les exigences règlementaires relatives au domaine d'activité d'OBSA, l'obligent à mettre en place des dispositifs de hautes précisions en matière de prévention et de protection contre l'incendie. Ainsi donc, Plusieurs dispositifs de prévention sont mises en place sur le site du terminal pétrolier et de la direction générale. Le plan d'opération interne du terminal d'Oryx Benin (POI) présente les différents scénarios en cas de déclenchement de feu. Les exercices de simulation d'incendie mensuels cumulés au plan de correction maintiennent un haut niveau d'alerte en la matière. Toutefois, il n'existe pas de système de détection et d'extinction automatique d'incendie, ce qui constitue une faille majeure. Les figure n°31 et n°32, présentent respectivement le plan du réseau incendie et une vue partielle d'un des nombreux rapports d'exercices de

simulation d'incendie étudié lors de cette étude. Le statut de probabilité affecté à la menace « Feu » est de trois (03).

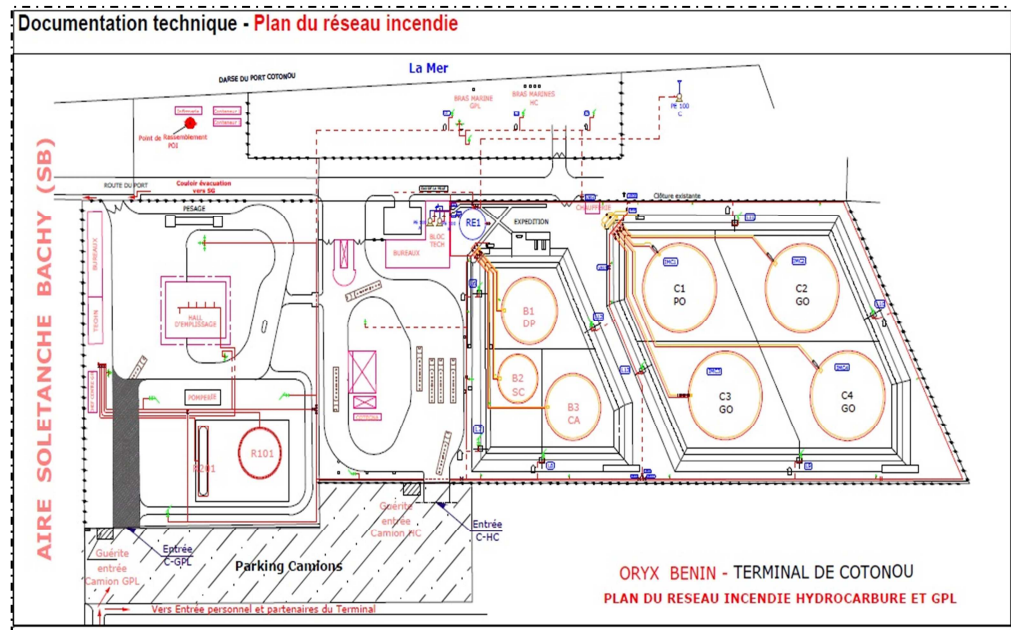


Figure n°31: Plan du réseau incendie d'OBSA

	<b>ORYX BENIN S.A.</b>					
	<b>RAPPORT EXERCICE INCENDIE</b>					
	Référence : B-QU-F-1-01-F	Version N° 1.00 du 15.02.2007				
<b>Scénario n° : 2012.07.02.n°006</b> <b>Date de l'exercice : 02/07/2012</b>						
<b>Thème :</b> «Au cours du déchargement du butane LPG, le joint reliant le Bras marine GPL et le manifold du Vessel céda, surgit une déflagration suivie d'une importante fuite ».						
<b>Personnels concernés par l'exercice :</b> <ul style="list-style-type: none"> <li>- <b>Etablissement :</b>            Tout le Personnel présent dans l'Etablissement :            Personnel OBSA ; Entreprises Extérieures, Chauffeurs et Visiteurs</li> <li>- <b>Secours extérieurs :</b>            Groupement National des Sapeurs Pompiers du PAC, attendu en vain.</li> </ul>						
<b>Description des circonstances du sinistre :</b> <ol style="list-style-type: none"> <li>1. <b>Lieu :</b> APB (Appontement pétrolier du Bénin).</li> <li>2. <b>Date et heure du sinistre :</b> 02/07/2012 à 16 h 45.</li> </ol> <b>Cause(s) :</b> <ol style="list-style-type: none"> <li>1. Vétusté du Joint.</li> <li>2. L'inattention des Opérateurs chargés de faire cette connexion (Ship and Shore).</li> <li>3. <b>Produit(s) concerné(s) :</b> (LPG) Butane.</li> <li>4. <b>Nature du (des) risque(s) :</b> <table style="display: inline-table; vertical-align: middle;"> <tr> <td><input checked="" type="checkbox"/> Sécurité des personnes</td> <td><input checked="" type="checkbox"/> Environnement</td> </tr> <tr> <td><input checked="" type="checkbox"/> Biens et Actifs</td> <td><input checked="" type="checkbox"/> Finance et Marketing</td> </tr> </table> </li> </ol>			<input checked="" type="checkbox"/> Sécurité des personnes	<input checked="" type="checkbox"/> Environnement	<input checked="" type="checkbox"/> Biens et Actifs	<input checked="" type="checkbox"/> Finance et Marketing
<input checked="" type="checkbox"/> Sécurité des personnes	<input checked="" type="checkbox"/> Environnement					
<input checked="" type="checkbox"/> Biens et Actifs	<input checked="" type="checkbox"/> Finance et Marketing					

Figure N°32: Extrait de Rapport d'exercice incendie

- **Explosions**

Des mesures préventives contre l'explosion sont mises en place au dépôt. Notamment les procédures sécuritaires et autres dispositifs électroniques de détection de fuite de gaz. La menace « explosion » est fortement prévenue et le niveau du statut de probabilité d'avènement de cette menace est de deux (2).

- **Terrorisme**

Etant situé dans la zone commerciale d'un pays de l'Afrique de l'Ouest et de surcroît, frontalier du Nigéria où sévissent des groupes terroristes de tous genres, la menace terroriste reste forte par défaut. OBSA n'a pris aucune disposition particulière en ce sens et les mesures dissuasives telle que la sécurité des accès, assurée par des agents de sécurités peu formés, rend cette menace encore plus probable. Le niveau du statut affecté à la probabilité d'avènement de cette menace est de quatre (04).

- **Produits Chimiques**

Le risque lié aux produits chimiques existe sur le site de la direction d'exploitation. Toutefois, l'existence d'un laboratoire en interne et les exigences réglementaire de l'ABE (Agence Béninoise de l'environnement) relève le niveau de prévention contre l'avènement d'une telle menace. Le niveau du statut de prévention contre la menace « produit chimique » est de deux (02).

- **Fumée**

Qu'elle soit produite par un incendie sur place ou poussée par le vent, l'effet toxique de la fumée reste très élevé, que ce soit pour l'homme à cause de l'intoxication à l'oxyde de Carbone (CO) et autres gaz (CO<sub>2</sub>, NH<sub>3</sub>, NO<sub>2</sub>...) tout aussi toxiques ou pour les équipements électroniques via des dépôts de microparticules affectant grandement leur fiabilité. Aucune disposition particulière n'a été prise pour prévenir l'avènement d'une telle menace quoi que peu probable dans un environnement comme celui étudié. Le niveau du statut de probabilité affecté à cette menace est de deux (02).



- **Grèves**

Le top management d'OBSA met un accent particulier sur la qualité du débat entre employeur et employés. La collaboration entre les délégués du personnel, les syndicats et les dirigeants permettant de résorber pacifiquement les potentiels foyers de tension. L'existence d'un accord d'entreprise et l'historique en matière de grève qui révèle « zéro grève » en 15 années d'existence, prouve bien que la menace « grève » est fortement prévenue. Le niveau du statut de probabilité affecté à cette menace est de deux (02).

- **Evènement Météorologique grave**

OBSA est situé au sud du Bénin où le climat est équatorial avec une forte humidité. Les violentes perturbations atmosphériques du genre cyclone extratropical ou la sécheresse y sont extrêmement rares. Outre les systèmes anti foudre, aucune disposition particulière n'est prévue face à l'avènement d'une telle menace. Le niveau du statut de probabilité affecté à ce sinistre est de deux (02).

- **Epidémies**

OBSA dispose d'un Service de médecine au travail qui assure la sensibilisation et le suivi sanitaire des employés sur le lieu de travail, et est garant de l'application des recommandations en cas d'alerte épidémie. Le dispositif de prévention face à la menace « Epidémie » est appréciable. Le statut de probabilité affecté à cette menace est de (02).

- **Inondation Internes**

Le risque d'inondation interne sur le site de la Direction d'Exploitation est élevé. Les canalisations hydrauliques sont en mauvais état et des salles d'eau jouxtent la salle informatique, sans oublier les travaux de constructions de nouveau qui bloquent la circulation de l'eau en temps de pluie. Le niveau du statut de probabilité affecté à la menace « inondation interne » est de quatre (04).

- **Vol/Brigandage**

L'accès aux sites du terminal pétrolier est uniquement contrôlé par des vigiles. Le risque que des personnes peu recommandables accèdent aux locaux est élevé. Le niveau de prévention de ce risque est donc faible et le statut du niveau de probabilité d'avènement affecté à cette menace est de trois (03).

- **Sabotage**

Les salles informatiques d'OBSA sont accessibles avec des clés ordinaires pouvant être falsifiées et aucune disposition d'ordre dissuasive (Caméra, accès électronique...etc.) n'existe. Le risque de sabotage reste alors élevé. Le statut du niveau de probabilité affecté à ce risque est de quatre (04).

- **Coupages de Courant**

Le Bénin n'est pas producteur d'énergie électrique. Il dépend des barrages hydroélectriques du Togo et du Ghana en termes d'énergie électrique. L'historique en matière de coupures électriques révèle des périodes de délestage ayant durée plusieurs jours. Toutefois OBSA dispose d'un réseau électrique stabilisé, ondulé et secouru par un groupe électrogène doté d'un système de démarrage automatique en cas de coupures. Le dispositif de prévention de la menace « coupures d'électricité » est bonne et le statut du niveau de probabilité y affecté est de un (01).

- **Coupure Internet**

La connexion par satellite qui nous permet à OBSA d'accéder à internet et implicitement, d'assurer l'interconnexion avec les autres sites du groupe ne dispose pas d'un backup de telle sorte qu'en cas de panne, la connexion à internet sera indisponible. Aucun dispositif de prévention contre la menace «coupure internet » n'existe et le niveau statut de potentialité affecté à cette menace est de quatre (04).

- **Coupures Téléphoniques**

Le risque lié aux coupures téléphoniques est géré chez OBSA. Un système de téléphonie GSM en corporate a été mis en place pour les employés ayant un besoin de communication élevé dans le cadre de leur activité. Toutefois, l'absence de ligne RTC, reste une faille à la Direction d'exploitation. Le niveau du statut de potentialité affecté à cette menace est de deux (02).

- **Négligences**

La probabilité d'avènement de la menace « négligence » est élevée chez OBSA. Cela est dû au fait que le personnel soit peu formé aux règlements d'usages acceptables du système d'information, mais également du fait de mauvaises connexions électriques et de l'état de la tuyauterie qui facilite l'accès des rongeurs aux locaux. Le niveau du statut de potentialité affecté à cette menace est de trois (03).

Le radar de la figure n°33 présente un récapitulatif des probabilités affectées suite à l'évaluation des mesures de prévention.

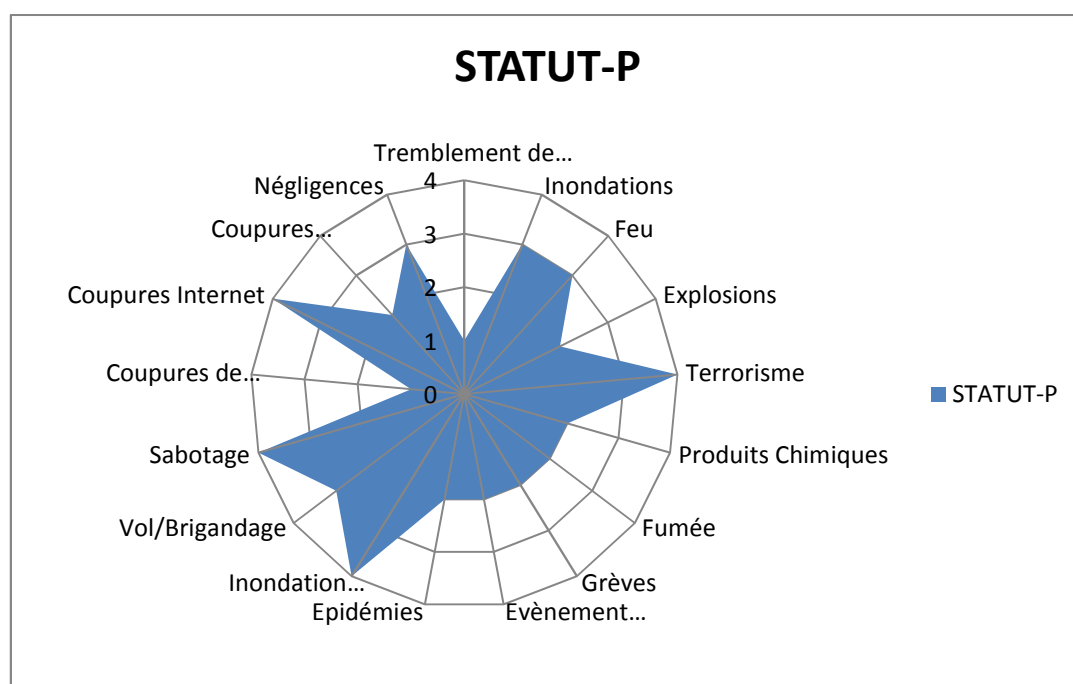


Figure n°33: Statut de potentialité

### **3.3.3.3. Etat de réduction des risques**

Une étude de l'environnement d'OBSA a révélé l'existence par défaut de mesures susceptibles de réduire l'impact potentiel en cas d'avènement et même la probabilité d'avènement de certaines des menaces ci-dessus présentées.

A cette étape, les différentes réunions de l'équipe projet ont permis d'évaluer le statut de réduction du risque en cas d'avènement de chacune des menaces. Le tableau XVII et le radar de la figure n°34 présentent la synthèse de l'évaluation des mesures de réduction du risque dans le contexte d'OBSA.

Menaces	STATUT-PRO	STATUT-PALL	STATUT-RECUP	Explication	STATUT-RI
Tremblement de terre	1	1	1	Aucunes mesures, ni de protection, ni palliative, ni de récupération contre le tremblement de terre n'a été mise en œuvre chez OBSA	1
Inondations	1	1	3	Aucune disposition particulière outre l'assurance n'a été prise pour la réduction de l'impact en cas d'avènement de ce sinistre	2
Feu	3	3	3	Les dispositions prises pour limiter l'impact en cas d'avènement de ce sinistre sont appréciables	3
Explosion	3	2	3	Il existe chez OBSA des mesures non négligeable de protection contre l'explosion.	3
Terrorisme	2	1	1	La problématique du terrorisme n'ayant pas été précédemment abordée par le management, aucune disposition particulière n'a été adoptée en ce sens.	1
Produit chimique	3	3	3	Le suivi rigoureux assuré par le laboratoire, l'alignement sur les exigences de l'ABE et d'autres dispositions interne au groupe rendent important l'effet de réduction de l'impact en cas d'avènement de cette menace.	3
Fumée	2	2	1	Aucune disposition n'a été prise dans ce cadre. Le dispositif de maîtrise est donc faible.	2
Grève	2	2	1	Quoique bien prévenu, l'impact d'une telle menace en cas d'avènement serait non négligeable du fait qu'un scénario pareil n'est pas été envisagé par le passé et qu'aucune disposition particulière n'ai été prise.	2

Evènement météorologique grave	1	1	1	Ce sont des évènements difficiles à prévoir, mais envisageables. Aucune disposition n'est prévue dans ce cadre. Le dispositif de maîtrise de ce risque est très faible.	1
Epidémies	3	2	1	OBSA dispose d'un Service de médecine au travail et les employés disposent d'une assurance maladie. Un bon dispositif de protection et de prévention existe donc.	2
Inondations interne	2	3	1	Le risque d'inondation est faible. Toutefois, les mesures prises pour qu'en cas de rupture de canalisation ou autres, l'impact du risque soit minimisé sont encore faibles.	2
Vol/Brigandage	2	1	2	La seule mesure de protection contre cette menace qu'est le contrôle d'accès assuré par des vigiles à l'entrée des locaux est plutôt moyen.	2
Sabotage	2	2	1	Aucunes dispositions susceptibles de limiter l'impact du sabotage n'a été mise en place chez OBSA.	2
Coupures de Courant	3	3	2	Les dispositions pour limiter l'impact de cette menace en cas d'avènement existent; toutefois les mesures de récupérations peuvent être améliorées	3
Coupures Internet	2	2	1	Aucune disposition en vue d'assurer la continuité de la communication internationale en cas de coupure internet n'existe. L'impact d'un tel sinistre dans le dans sera insupportable.	2
Coupures Téléphoniques	3	4	2	L'impact de l'avènement d'un tel scénario sera relativement faible donnée les bonnes mesures de protection et palliatives mises en place	3
Négligences	2	3	1	Le risque lié à la négligence est élevé. Le niveau de formation aux usages acceptables du SI est très faible.	2

Tableau XVII: Etat de réduction des impacts des sinistres

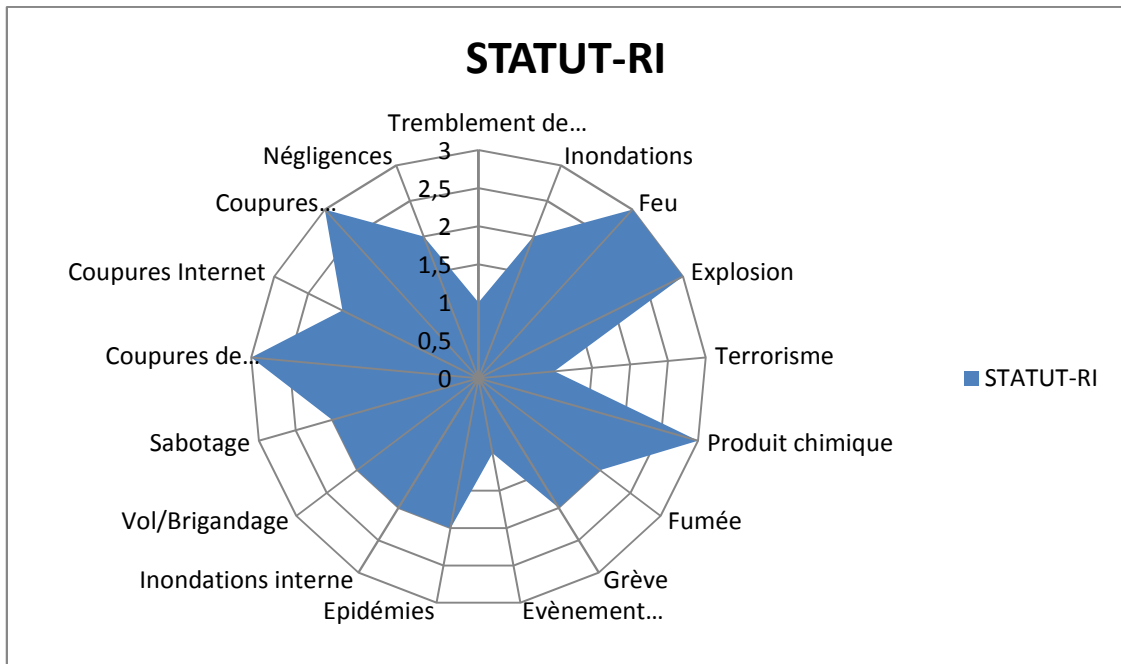


Figure n° 34: Statut de réduction du risque

### 3.3.3.4. Priorisation des scénarios de sinistre

La grille de classification des sinistres ci-dessous présentée (Tableau XVIII) dont le principe directeur a été d'envisager l'impact extrême en cas d'avènement de chaque des sinistres a été validé par le comité de pilotage.

Menaces	Niveau de priorité
Fumée	1
Coupures de Courant	
Grèves	
Epidémies	
Coupures Téléphoniques	2
Produits Chimiques	
Négligences	
Coupures Internet	3
Sabotage	
Inondation Internes	
Vol/Brigandage	
Terrorisme	
Feu	4
Explosions	
Evènement Météorologique graves	
Inondations	

Tableau XVIII: Priorisation des scénarios de sinistre

### 3.3.3.5. Evaluation des impacts

Le croisement entre le statut de réduction du risque et la grille de priorisation des menaces a permis d'évaluer le statut de l'impact potentiel des scénarios tel que présenté par le tableau XIX, sur la base de la matrice de la figure n°35 qui présente par statut de réduction de risque et priorisation de menace, l'impact potentiel des menaces.

Menaces	Niveau de priorité	STATUT-RI	IMPACT
Coupures de Courant	1	3	1
Coupures Téléphoniques	1	2	
Epidémies	1	3	
Fumée	1	2	
Grèves	1	1	
Coupures Internet	2	3	2
Négligences	2	3	
Produits Chimiques	2	2	
Feu	3	3	
Inondations Internes	3	2	3
Sabotage	3	2	
Terrorisme	3	2	
Vol/Brigandage	3	2	
Tremblement de terre	3	2	
Evènement Météorologique graves	4	2	
Explosions	4	1	4
Inondations	4	1	

Tableau XIX : Impact des menaces

Priorisation des menaces STATUT-RI	Priorisation des menaces			
	1	2	3	4
1	1	2	3	4
2	1	2	3	3
3	1	2	2	2
4	1	1	1	1

Figure n°35: Grille d'évaluation d'impact



La grille d'évaluation de l'impact a permis d'identifier quatre grandes catégories de menaces en terme d'impact tel qu'illustré par le radar de la figure n°36.

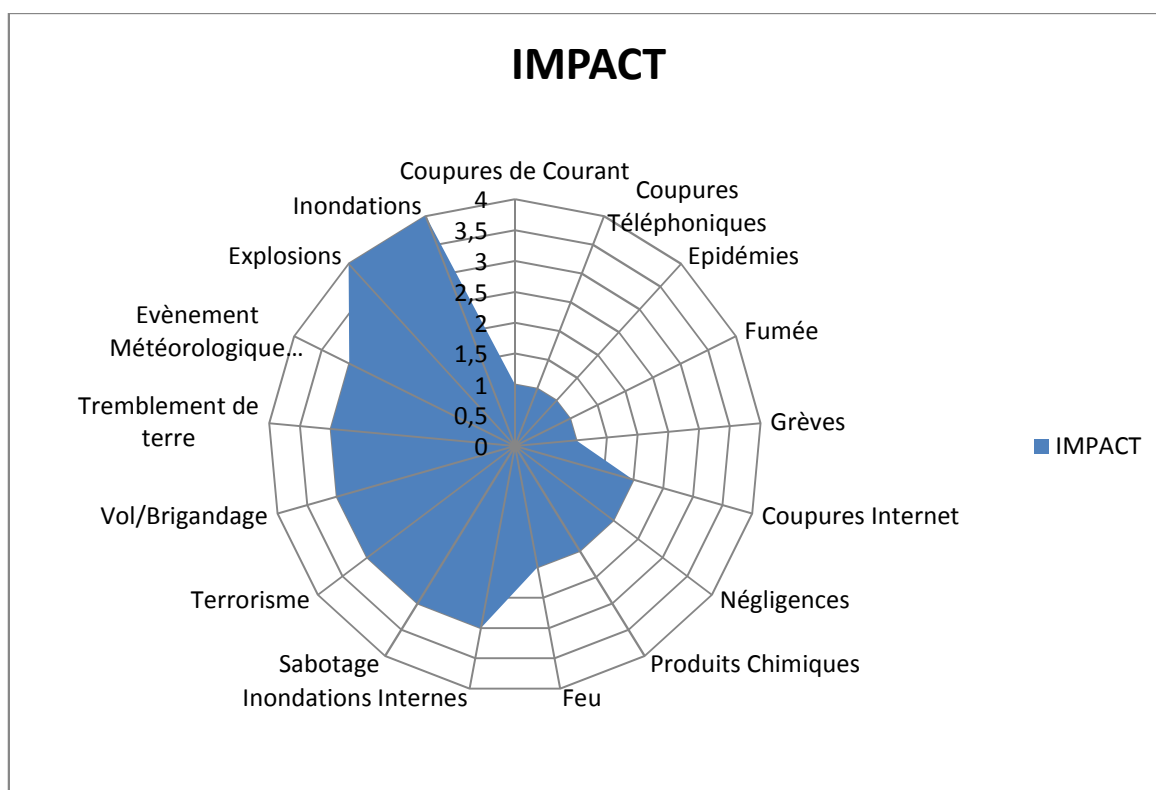


Figure n°36: Impact des menaces

On distingue :

- Le groupe n°1, des menaces à impact insignifiant, encadré en noir et constitué de:
  - Coupure de courant
  - Coupures téléphoniques
  - Epidémie
  - Fumée
  - Grèves
  
- Le groupe n°2, des menaces à impact toléré, encadré au vert et constitué de:
  - Coupure internet
  - Négligences
  - Produits chimiques
  - Feu
  
- Le groupe n°3, des menaces à impact inadmissible, encadré au jaune et constitué de:

- Inondations internes
  - Sabotage
  - Terrorisme
  - Vol/brigandage
  - Tremblement de terre
  - Evènement Météorologique grave
- Le groupe n°4 des menaces à impact insupportable, encerclé au rouge et constitué de :
- Explosion
  - Inondation

### 3.3.3.6. Sévérité du risque

Le tableau XX, issu du croisement entre la figure n°36 et la grille d'aversion aux risques illustrée par la figure n°28 a permis de ressortir les niveaux de risque.

Menaces	IMPACT	STATUT-P	Niveau de risque
Coupures de Courant	1	1	● 0
Coupures Téléphoniques	1	2	
Epidémies	1	2	
Fumée	1	2	
Grèves	1	2	
Produits Chimiques	2	2	● 2
Feu	2	3	
Négligences	2	3	
Tremblement de terre	3	1	● 3
Coupures Internet	2	4	
Evènement Météorologique graves	3	2	
Vol/Brigandage	3	3	
Inondations Internes	3	4	
Sabotage	3	4	
Terrorisme	3	4	● 4
Explosions	4	2	
Inondations	4	3	

Tableau XX: Sévérité du risque

### **3.3.3.7. Choix des menaces à étudier**

L'identification de ces menaces constitue le point d'entrée de l'analyse d'impact sur l'activité (BIA), qui permettra sur la base de ces menaces, d'identifier les processus critiques, ainsi que les objectifs de reprise en termes de temps. Les scénarios de menace retenus sont ceux ayant un niveau de risque 3 et 4; à savoir:

- Coupure internet
- Evènement météorologique grave
- Vol/Brigandage
- Inondations internes
- Sabotage
- Terrorisme
- Explosions
- Inondations

L'étude d'impact sur l'activité et implicitement l'analyse de risque se sont basées sur ces huit menaces.

### 3.4. Analyse d'impact sur l'activité

Le déroulement de l'analyse d'impact s'est basé dans un premier temps sur une série d'interviews BIA, ensuite, les informations issues de ces interviews ont été apurées, puis synthétisées, afin d'en extraire les outputs du BIA.

Je présente ci-dessous le processus BIA tel qu'il s'est déroulé, et une synthèse des informations constituant la matrice BIA.

#### 3.4.1. Interviews BIA

L'objectif premier des interviews BIA a été de recenser le maximum d'information auprès des utilisateurs en vue de déterminer avec le plus haut niveau de précision possible, les objectifs en temps de reprise, les ressources clés et les impacts des sinistres sur l'activité.

#### 3.4.2. Identification des activités

Le découpage du système d'information établi à la figure n°23 mettant en évidence les différentes activités supportées par le SI, constitue un point d'entrée à l'exécution de cette étape de l'analyse d'impact sur l'activité et inscrit OBSA dans le contexte suivant:

L'entreprise présente ses activités de manière simple et succincte. Elle a réalisé un premier niveau d'organigramme indiquant qui est responsable de quelle activité. En revanche, il n'existe aucune liste de ce qui pourrait être critique dans ses activités. Pour commencer l'analyse d'impact, on s'adressera donc aux responsables désignés.

Les processus à étudier sont ceux supportés par les SI opérationnel et d'aide à la décision, ci-dessous présentés par le tableau XXI.

Fonction	Processus métier
Opérateur	Confirmer chargement
	Elaborer point de chargement
	Libérer camion
Administration des ventes	Gérer commande client
	Gérer logistique
	Elaborer Point des commandes

Comptabilité client	Gérer facturation client
	Elaborer Reporting compta client
	Mettre à jour fichier client
	Libérer commande
Comptabilité Fournisseur	Gérer facture fournisseur
	Elaborer Reporting compta fournisseur
	Gérer situation fournisseur
Comptabilité Matière	Gérer stock
	Elaborer stock report
Comptabilité Générale	Elaborer budget
	Gérer immobilisation
	Paramétrer comptes
	Gérer fiscalité
GRH	Gérer Paie
	Gérer temps de travail
	Gérer ressources externes
	Gérer carrière
Contrôle de gestion	Gérer KPI
	Contrôler Reporting
	Gérer Capex report
Reporting et consolidation	Gérer consolidation
	Elaborer Reporting

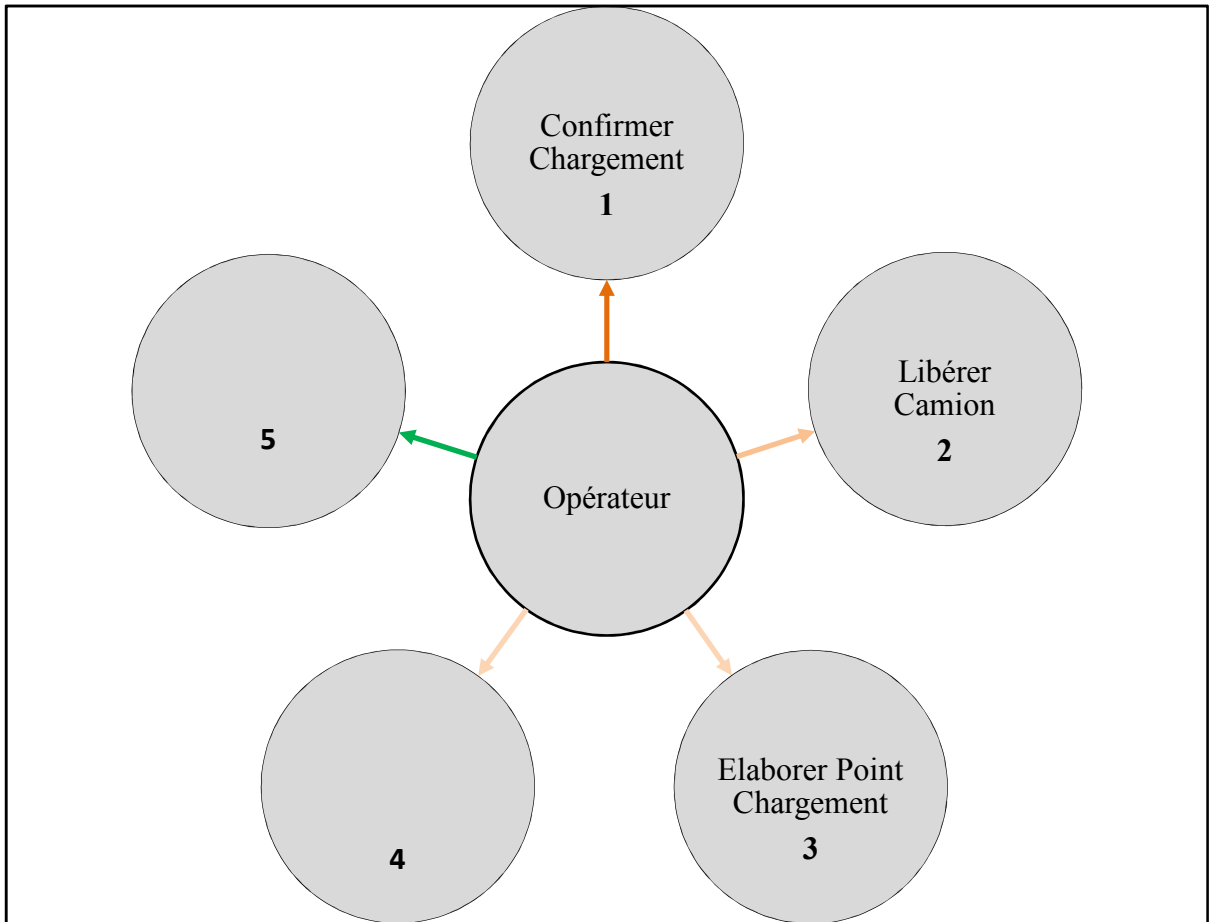
Tableau XXI: Processus étudiés

### 3.4.3. Classification des processus

Chaque responsable de service a procédé à une hiérarchisation en terme de priorités, des processus exécutés au titre de sa fonction; lesquels processus ont été ensuite analysés pour en identifier les livrables, et y affecter un niveau de criticité.

Je présente ci-dessous, la classification des processus relatifs à la fonction « opération », suivant le paradigme introduit par l'interview BIA, tel que réalisé lors des interviews.

Quel est en termes de priorité, les processus que vous exécutez au quotidien dans l'exercice de votre fonction ?



Analyse des processus critiques			
Réf	Nom du Processus	Livable	Niveau de Priorité
1	Confirmer Chargement	Bulletin de livraison	CRITIQUE
2	Libération Camion	Fiche de Libération Camion	IMPORTANT
3	Elaborer point	Rapport d'activité	NECESSAIRE
4			
5			
<b>CRITIQUE</b>		Relatif aux processus le plus critique de la fonction, dont l'indisponibilité affecterait à l'extrême la fonction	
<b>IMPORTANT</b>		Relatif au processus de criticité moyenne, dont l'indisponibilité n'affectera la fonction que dans le temps	
<b>NECESSAIRE</b>		Processus dont l'indisponibilité n'affectera que de façon très infime la fonction	

Cette première série d'interviews a permis de caractériser le niveau de criticité des processus.

### 3.4.4. Analyse détaillée des processus

Il a été retenu d'étudier les processus ayant un niveau de priorité marqué soit « CRITIQUE » ou soit « IMPORTANT ». Ci-dessous la présentation du déroulement de cette étape pour la fonction « Opérateur ».

Description du Processus			
REF	Nom du Processus	Livrable	Niveau de priorité
1	Confirmer Chargement	Bulletin de livraison	CRITIQUE
Résumé		Réception de la demande de chargement	
		Vérification du statut de chargement	
		Confirmation chargement	
Sous processus			
Responsable du processus		Chef Equipe	
Processus précédent lié		Gérer commande Client	
Existe-t-il un processus alternatif ?		Non	
Organigramme du processus		<pre> graph TD     DEBUT([DEBUT]) --&gt; Dem[Demande de chargement]     Dem --&gt; Stat{Statut = 30}     Stat -- Non --&gt; Dem     Stat -- Oui --&gt; Conf[Confirmer Chargement]     Conf --&gt; BL[/Consulter BL/]     BL --&gt; FIN([FIN])         </pre>	

Description du Processus			
REF	Nom du Processus	Livrable	Niveau de priorité
2	Libérer Camion	Fiche de libération	Important
Résumé		Réception demande de libération	
		Consulter numéro BL	
		Libérer Camion	
Sous processus			
Responsable du processus		Chef Equipe	
Processus précédent lié		Confirmer Chargement	
Existe-t-il un processus alternatif ?		Non	
Organigramme du processus		<pre> graph TD     DEBUT([DEBUT]) --&gt; Input[/Demande de Libération/]     Input --&gt; Decision{Statut &gt; 50}     Decision -- Non --&gt; Input     Decision -- Oui --&gt; Action1[Libérer Camion]     Action1 --&gt; Action2[Imprimer fiche]     Action2 --&gt; FIN((FIN)) </pre>	



### 3.4.5. Identification des ressources

Il s'est agi à cette phase de l'interview, d'identifier les ressources nécessaires au fonctionnement des processus, suivant les scénarios nominaux. Le cas de la fonction « Opérateur » est présenté ci-dessous.

Ressources normalement utilisées par la fonction opérateur			
Nombre des membres de l'équipe	Quatre (04)		
Outil: spécifiques ou rares	Imprimante Matricielle Papier Listing	Nécessité d'un outil rare	<input checked="" type="checkbox"/>
Personnes clés ou intérimaires	1	Nom	Fanou Jean Marie
	2	Nom	Avidjè Pierre
	3	Nom	Cyriaque Agnoun
Poste de travail	<ul style="list-style-type: none"> <li>• Ordinateur de bureau</li> <li>• Imprimante matricielle</li> <li>• Papier listing</li> <li>• Poste téléphonique</li> <li>• ERP JDE</li> <li>• Suite MS Office</li> </ul>		
Accès internet	Non		
Spécialiste de l'application informatique	Francis Yelouassi		
Spécialiste du matériel	Alidou Chabi Gani		
Document vitaux	Informations de jaugeage Table de barémage Dossier Gestion stock		
Autres matériel vitaux			
Emplacement	Direction d'exploitation		

### 3.4.6. Evaluation des impacts

Cette étape de l'interview a permis de recenser les informations relatives aux éventuels impacts sur l'entreprise, en cas de perturbation du cours normal des processus étudiés. Ci-dessous illustré, les implications du dysfonctionnement de la fonction « Opérateur », telle que présenté lors des interviews BIA.

En cas de perturbation			
Quand est – ce que les clients constaterons la perturbation	24H	Impact potentiel	Arrêt des opérations
Quand est ce que les fournisseurs constaterons la perturbation	En temps réel	Réaction potentielle	Retour des camions
Quelles autres conséquences	<ul style="list-style-type: none"> <li>• Intégrité des personnes et des biens</li> <li>• Image</li> <li>• Financier</li> </ul>		<ul style="list-style-type: none"> <li>• Impact de niveau 5 sur l'image</li> <li>• 2.500.000 XOF par jour</li> <li>• Pas d'impact sur l'intégrité des personnes et des biens</li> </ul>

### 3.4.7. Evaluation des objectifs en temps de reprise

Cette phase a permis de recenser les contraintes et exigences relatives aux processus et accompagner les utilisateurs dans l'estimation des objectifs en temps de reprise. Ci-dessous, le cas de la fonction « opérateur ».

Exigences		
Conformité		
Règlementaire ou contractuel	Livraison du client sous 24H dès réception de la demande	
Statutaire		
Réciproque (Fournisseur)		
Environnemental		
Durée d'interruption maximale acceptable		
MTD	Limite	
RTO	Temps	
RPO	Donnée	
Livrables exigibles à dates clés		
Livable	Date et heure de transmission	Impact en cas de non transmission
Bulletin de livraison	Tous les jours à 16H	Elevé
Fiche de Libération Camion	Tous les deux jours avant 16H	Elevé
Rapport d'activité	Chaque fin de mois	Faible

### 3.4.8. Fonctionnement en mode dégradé.

Cette phase a permis d'identifier en fonction de leur criticité, les ressources nécessaires au fonctionnement en mode dégradé des processus. Ci-dessous, le cas de la fonction « Opérateur »

Ressources utilisées par la fonction en mode dégradé								
Type de ressource	Laps de temps					Impact si indisponible		Arrangement d'urgence
	1H	4H	1J	1M	1A	Faible	Elevé	Ressource externes
Personnes clés ou intérimaires						<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Poste de travail						<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Accès internet						<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Spécialiste de l'application informatique						<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Spécialiste du matériel						<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Document vitaux						<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Autres matériels vitaux						<input type="checkbox"/>	<input type="checkbox"/>	
Emplacement						<input type="checkbox"/>	<input checked="" type="checkbox"/>	

### 3.4.9. Synthèse de l'interview BIA

La synthèse des informations recueillies au cours des interviews sus-présentées a permis de produire sous forme de tableaux synthétiques, les outputs attendus du BIA à savoir:

- La classification des processus
- Les impacts financiers et opérationnels
- Les processus critiques
- Les configurations (MTD, WRT)
- Les applications et systèmes informatiques critiques
- Les objectifs en temps de reprise (RPO et RTO)

Je présente ci-dessous les tableaux d'impacts financiers et opérationnels, des configurations et des objectifs en temps de reprise. Le reste des tableaux sont annexés au présent document.

▪ **Tableaux d'impacts financiers et opérationnels**

Le tableau XXII ci-dessous, présente les impacts financiers et opérationnels.

Fonction	Processus métier	Priorité	Perte quotidienne	Impact de la perte			Note final
				Chiffrage perte quotidienne	Image	Revendeur	
Opérateur	Confirmer chargement	CRITIQUE	2500000	3	3	3	15
	Libérer camion	CRITIQUE	1500000	3	3	3	15
Administration des ventes	Gérer commande client	CRITIQUE	2500000	3	3	3	15
	Gérer logistique	CRITIQUE	1000000	2	2	2	10
Comptabilité client	Gérer facturation client	CRITIQUE	3500000	3	2	1	11
	Mettre à jour fichier client	CRITIQUE	2000000	3	2	2	12
	Libérer commande	CRITIQUE	1000000	2	3	1	11
Comptabilité Fournisseur	Gérer facture fournisseur	CRITIQUE	1000000	3	2	0	10
Comptabilité Matière	Gérer stock	IMPORTANT	2000000	3	0	2	8
	Elaborer stock report	IMPORTANT	75000	0	0	0	0
Comptabilité Générale	Paramétrer comptes	CRITIQUE	80000	0	0	1	1
	Gérer fiscalité	CRITIQUE	350000	0	0	0	0
GRH	Gérer Paie	IMPORTANT	2000000	3	2	0	10
Reporting et consolidation	Gérer consolidation	CRITIQUE	150000	3	2	0	10
	Elaborer Reporting	CRITIQUE	150000	3	3	0	12
Coefficient				2	2	1	

Tableaux XXII: Impacts financiers et opérationnels

▪ **Processus critiques**

Il a été reconnu comme étant critiques, les processus ayant une Gravité supérieure ou égale à 10. Le tableau XXIII présente les processus critiques.

Fonction	Processus métier	Gravité
Opérateur	Confirmer chargement	15
	Libérer camion	15
Administration des ventes	Gérer commande client	15
	Gérer logistique	10
Comptabilité client	Gérer facturation client	11
	Mettre à jour fichier client	12
	Libérer commande	11
Comptabilité Fournisseur	Gérer facture fournisseur	10
GRH	Gérer Paie	10
Reporting et consolidation	Gérer consolidation	10
	Elaborer Reporting	12

Tableau XXIII: Processus Critiques

▪ **configurations**

Le tableau XXIV, ci-dessous, met en évidence, les configurations, à savoir :

- La durée maximale tolérable d'interruption de l'activité
- Les priorités pour les actions de reprises.

Fonction	Processus métier	Gravité	MTD (en jours)	Ordre de priorité
Opérateur	Confirmer chargement	15	1	1
	Libérer camion	15	1	1
Administration des ventes	Gérer commande client	15	0,5	1
	Gérer logistique	10	1	1
Comptabilité client	Gérer facturation client	11	1	1
	Mettre à jour fichier client	12	1	2
	Libérer commande	11	0,5	1
Comptabilité Fournisseur	Gérer facture fournisseur	10	2	2
GRH	Gérer Paie	10	5	1
Reporting et consolidation	Gérer consolidation	10	2	2
	Elaborer Reporting	12	1	1

Tableau XXIV: Configurations

- **RTO**

Le tableau XXV, ci-dessous, met en exergue le RTO et WRT des processus métiers critiques.

<b>Fonction</b>	<b>Processus métier</b>	<b>RTO</b>	<b>WRT</b>
Opérateur	Confirmer chargement	1,5	1
	Libérer camion	1,5	0,5
Administration des ventes	Gérer commande client	1,5	1
	Gérer logistique	1,5	0,5
Comptabilité client	Gérer facturation client	1,5	1,5
	Mettre à jour fichier client	1,5	0,5
	Libérer commande	1,5	0,5
Comptabilité Fournisseur	Gérer facture fournisseur	1,5	1
GRH	Gérer Paie	1	0,5
Reporting et consolidation	Gérer consolidation	3	1
	Elaborer reporting	1	1

Tableau XXV: RTO

- **Détermination du RPO**

Le tableau XXVI récapitule, le calcul du RTO. Souvenons-nous:  $RPO = RTO - WRT$

<b>Application et systèmes critiques</b>	<b>RPO (en jour)</b>
ERP JDE sur le site de la Direction d'exploitation	0,5
ERP JDE sur le site de la Direction Générale	1
Logiciel Sage Saari	1
Logiciel Vigilens	1
Système d'automatisation Alma sur site de la Direction d'exploitation	0,5
Téléphonie	1

Tableau XXVI: Détermination du RPO

### 3.5. Analyse de risque

L'analyse de risque s'est basée sur les processus critiques, issues de l'analyse d'impact sur l'activité, avec pour objectif de définir des plans de réduction des risques d'avènement des menaces retenues à l'issue de la cartographie des sinistres. Les critères retenus sont:

- D: Disponibilité
- I : Intégrité
- C: Confidentialité

L'outil méthodologique Méhari a été utilisé pour réaliser l'analyse de risque. En effet, ce dernier intègre bien les critères, ci-dessus présentés, est dédié aux risques liés à l'information et enfin, la disponibilité d'une base de connaissance permettant une analyse complète de risque a justifié ce choix.

Dans ce sous chapitre, je présente brièvement au prime abord l'outil utilisé pour réaliser l'analyse de risque, ensuite je présente le déroulement de l'analyse de risque et ses «outputs ».

#### 3.5.1. Base de connaissance Méhari

La base de connaissance MEHARI 2010 2.14, distribuée par le CLUSIF propose une méthodologie d'analyse, d'évaluation et de gestion des risques liés à l'information et à son utilisation.

Cette base de connaissance disponible sous forme d'un classeur Excel, dont l'écran d'accueil est présenté à la figure n°37 et dont le schéma de navigation est illustré par la figure n°38 est constituée de trente-cinq (35) feuilles classées en six groupes avec comme objectifs:

- Mise en œuvre générale : Intro, Dossier, Nav, License
- Paramétrage de la méthode : Vulnérabilité Type, Grille IP, Gravité
- Analyse des enjeux et classification des actifs : T1, T2, T3, Classif
- Diagnostique des services de sécurité : 01 Org à 14 ISM, Service, Thèmes, Score ISO
- Evaluation des risques : Expo, Scénarios, Risk%actif, Risk%event
- Préparation de plan : Plan\_Action, Obj\_PA, OBJ\_Projets

Onglet	Objectif	
Intro	Description et navigation entre les onglets du fichier de la base de connaissance	
Dossier	Description du contexte de réalisation du dossier	
Nav	Schéma de navigation dans la base de connaissance	
Licence	Rappel de la licence Publique de MEHARI	
<b>Module d'analyse des enjeux et classification des actifs:</b>		
T1, T2 et T3	Tableaux de classification	Tableaux de classification : T1, T2, T3 et Classif → Masquer <input type="checkbox"/>
Classif	Classification des actifs	
<b>Module du diagnostic des services de sécurité (ou d'audit)</b>		
Domaines 01 Org à 14 MSI	Questionnaires relatifs aux domaines (01 à 14) de sécurité MEHARI	Feuilles de questionnaires : de 01Org à 14 Msi Thèmes et Score ISO → Masquer <input type="checkbox"/>
Services	Récapitulé de la qualité des services de sécurité (avec variantes)	
Thèmes	Thèmes de sécurité Mehari : regroupement des services et sous-services en 10 centres d'intérêts et 18 axes de représentation	
Score ISO	Table de scoring ISO 27002 suite au diagnostic des services Mehari	
<b>Module d'analyse de risque (identification, estimation et évaluation des risques)</b>		
Expo	Tableau des expositions naturelles aux menaces	Feuilles d'analyse des risques : Evénements types, Risques par actifs ou événements → Masquer <input type="checkbox"/>
Scénarios	Scénarios de risque incluant le calcul des risques	
Risk%Actif	Panorama de gravité des scénarios par type d'actif	
Risk%event	Panorama de gravité des scénarios par type d'événement	
<b>Traitement des risques : options, plans de réduction et suivi</b>		
Plans_action	Sélection de plans de réduction des risques	Feuilles de traitement : Plans_d'action Obj_PA → Masquer <input type="checkbox"/>
Obj_PA	Sélection de plans de réduction des risques	
Obj_Projets	Sélection de plans de réduction des risques	
<b>Éléments permanents et de paramétrage de la méthode</b>		
Vulnérabilités types	Les onglets qui suivent sont apportés avec la méthode	Feuilles des vulnérabilités types, Grilles d'acceptabilité des risques et d'évaluation de I et P, Corr_Services → Masquer <input type="checkbox"/>
Gravité	Détermination de la Gravité du risque en fonction de la Potentialité et de l'Impact	
Grilles IP	Tables de détermination d'Impact et de Potentialité des scénarios	
Corr_Services	Table de correspondance entre les services de Mehari 2010 et ceux de la version 2007	

Figure n°37: Page d'accueil Méhari

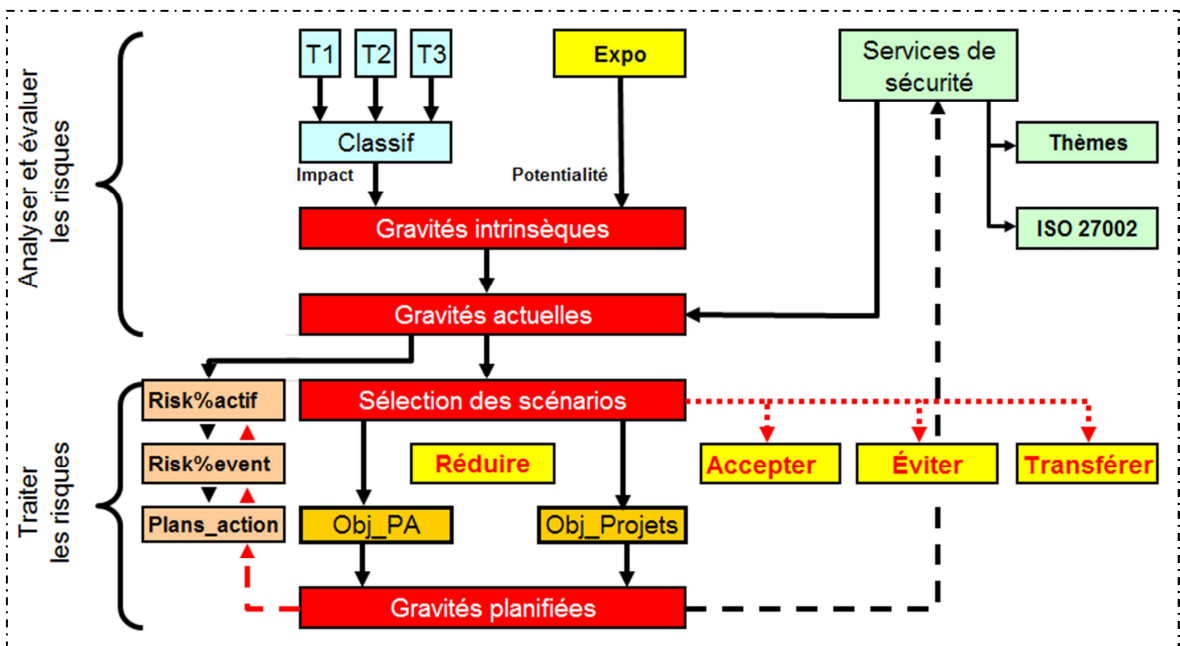


Figure n°38: Schéma de navigation - Méhari

### 3.5.2. Classification avec Méhari

A cette étape, l'exploitation de la base de connaissance a consisté au renseignement des informations de classification des données et des services, par processus critique. Il



en ressort une classification pour le périmètre ainsi défini. La figure n°39 (ci-dessous), illustre un aperçu de la classification des services.

Tableau T2  Processus métier, application ou domaine applicatif  Services communs	CLASSIFICATION DES SERVICES																	
	Services du réseau étendu		Services du réseau local		Services applicatifs			Services bureautiques communs		Equipe-ments mis à la disposition des utilisateurs	Services systèmes Communs (Systèmes, périfs, etc.)		Services de publication sur site web		Services généraux environnement de travail	Services télécom		
	D	I	D	I	D	I	C	D	I	D	D	I	D	I	D	D	I	
Nom de colonne pour formules Classif	R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S04	S04	S05	S05	G01	G02	G02	
<b>Processus métiers</b>																		
Domaine 1 : Confirmer Chargement	2	1	4	3	4	4	2	3	1	4	4	1	1	1	2	3	1	
Domaine 2 : Libérer Camion	2	1	4	3	4	4	2	2	1	4	3	1	1	1	2	3	1	
Domaine 3 : Gérer commande client	2	1	4	3	4	4	2	2	2	4	1	1	1	1	2	3	3	
Domaine 4 : Gérer logistique	2	1	4	3	2	4	2	4	3	4	1	1	1	1	2	3	2	
Domaine 5 : Gérer facturation client	3	1	4	3	4	4	2	3	3	4	4	1	1	1	2	3	2	
Domaine 6 : Mettre à jour fichier client	2	1	4	3	4	4	2	1	1	4	1	1	1	1	2	3	1	
Domaine 7 : Libérer commande	2	1	4	3	4	4	2	1	1	4	1	1	1	1	2	3	2	
Domaine 8 : Gérer facture fournisseur	3	1	3	2	4	4	2	3	4	4	3	1	1	1	2	3	2	
Domaine 9 : Gérer paie	1	1	2	2	4	4	4	3		4	3	1	1	1	2	3	1	
Domaine 10 : Gérer Consolidation	4	3	3	4	4	4	4	4	3	4	2	1	1	1	2	4	3	
Domaine 11 : Elaborer reporting	4	3	3	4	3	4	4	4	3	4	3	1	1	1	2	4	3	
<b>Processus transverses</b>																		
Processus 1 :																		
Processus 2 :																		
Processus 3 :																		
Administration/ politique d'ensemble																		
Classification pour l'ensemble	4	3	4	4	4	4	4	4	4	4	4	1	1	1	2	4	3	

Figure n°39: Classification des services

L'étape de classification a permis d'obtenir la table des impacts intrinsèque. Le critère D (disponibilité) a été déterminant dans la sélection des actifs à intégrer au scoop du plan de continuité.

La figure n°40 ci-dessous illustre par le tableau d'impacts intrinsèques ainsi que la sélection des actifs devant appartenir au scope du plan de continuité.

Tableau d'Impact Intrinsèque				Sélection d'actifs	
Actifs de type Données et informations					
	D	I	C		
<b>Données et informations</b>					
D01	Fichiers de données ou bases de données applicatives	4	4	4	1
D02	Fichiers bureautiques partagés	4	3	1	1
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)	1	1	1	0
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles	1		1	0
D05	Listings ou états imprimés des applications informatiques			3	0
D06	Données échangées, écrans applicatifs, données individuellement sensibles	1	1	1	0
D07	Courrier électronique	3	3	4	1
D08	Courrier postal et télécopies	1	1	1	0
D09	Archives patrimoniales ou documentaires	1		1	0
D10	Archives informatiques	3	3	3	1
D11	Données et informations publiées sur des sites publics ou internes	1	1	1	0
<b>Actifs de type Services</b>					
	D	I	C		
<b>Services généraux communs</b>					
G01	Environnement de travail des utilisateurs	2			0
G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)	4	3		1
<b>Services informatiques et réseaux</b>					
R01	Service du réseau étendu	4	3		1
R02	Service du réseau local	4	4		1
S01	Services applicatifs	4	4	4	1
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	4	4		1
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	4			0
<b>Nota : Considérer ici la perte massive de ces services et non celle d'un seul utilisateur</b>					
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.	4	1		0
S05	Services de publication d'informations sur un site web interne ou public	1	1		0

Figure n°40: Impact intrinsèque

### 3.5.3. Audit de l'existant

L'audit de l'existant via Méhari s'est basé sur les éléments ci-dessous:

- La phase d'audit de l'existant a porté sur:
- La sécurité des sites
- La sécurité des locaux
- Le réseau WAN
- Le réseau LAN
- L'exploitation des réseaux
- La sécurité des systèmes et leur architecture
- La production informatique
- L'exploitation des télécommunications

Cette analyse a été facilitée par la décomposition cellulaire suivante:

Entité : Oryx Bénin SA

- Locaux:
  - Local Technique Direction Générale
  - Local Technique Dépôt GPL
  - Local technique Dépôt HC

- Architecture réseaux et télécom :
  - Réseau Local Direction Générale
  - Réseau Local Dépôt GPL
  - Réseau Local Dépôt
  
- Exploitation réseaux et télécom:
  - Exploitation réseaux et télécom
  
- Architecture des systèmes
  - Server de Backup
  - Server JDE Production
  - Server JDE Déploiement
  - Server de Messagerie Lotus Domino
  
- Production Informatique  
Exploitation des servers pour la mise à disposition de ressource
  
- Application opérationnelle
  - ERP JDE
  - Application Vigilens
  - Application HFM
  - Suite Microsoft Office
  - Sage Saari

Les séries de questionnaires d'audit proposées par Mehari, nous avons retenu celles qui traitent des aspects relatifs à la continuité de chacun des éléments concernés. En effet, Mehari offre la latitude de circonscrire, le périmètre des scénarios de crise. La figure n°41 ci-dessous donne un aperçu des questionnaires relatifs à la continuité et retenu afin d'évaluer le dispositif de continuité existant.

<b>05A04</b>	<b>Procédures et plans de reprise du réseau local sur incidents</b>		
05A04-01	A-t-on établi une liste des incidents pouvant affecter le bon fonctionnement du réseau local et analysé la criticité de chacun d'eux ?	0	
05A04-02	A-t-on établi, pour chaque incident critique, la solution à mettre en oeuvre et les opérations à mener par le personnel d'exploitation ?	0	
05A04-03	Les moyens d'intervention sur le réseau local (tant de diagnostic que de reconfiguration) couvrent-ils de manière satisfaisante tous les cas de figures analysés et permettent-ils de mettre en oeuvre les solutions décidées dans les délais spécifiés ?	0	
05A04-04	A-t-on défini, pour chaque incident critique du réseau local, un délai de résolution et une procédure d'escalade en cas d'insuccès ou de retard des mesures prévues ?	0	
05A04-05	Les moyens de diagnostic et de pilotage et de reconfiguration du réseau sont-ils protégés contre toute inhibition intempestive ou malveillante ?	0	
05A04-06	Les procédures de reprise sur incident tiennent-elles compte d'une éventuelle perte de données (en particulier perte de	0	
05A04-07	Audite-t-on régulièrement la capacité des moyens de diagnostic et de reconfiguration à assurer un fonctionnement minimal du réseau satisfaisant en cas d'incident ?	0	
<b>05A05</b>	<b>Plan de sauvegarde des configurations du réseau local</b>		
05A05-01	A-t-on établi un plan de sauvegarde, couvrant l'ensemble des configurations du réseau local, définissant les objets à sauvegarder et la fréquence des sauvegardes ?	0	
05A05-02	Ce plan de sauvegarde est-il traduit en automatismes de production ?	0	
05A05-03	Teste-t-on régulièrement que les sauvegardes des programmes (sources et/ou exécutables), de leur documentation et de leur paramétrage permettent effectivement de reconstituer à tout moment l'environnement de production ?	0	
05A05-04	Les automatismes de production assurant les sauvegardes sont-ils protégés par des mécanismes de haute sécurité contre toute modification illicite ou induite ?	0	

Figure n°41: Extrait du questionnaire d'audit

### 3.5.4. Gravité des scénarios par type d'actif et par type d'évènement

Le panorama des gravités par scénario a ainsi permis d'identifier par rapport au critère de disponibilité (D), le nombre exact et le degré de gravité par type d'actif. On recense donc, par exemple, deux (02) actifs de seuil de gravité 4 pour les actifs du type « Données et information » et neuf (09) actifs de seuil de gravité 4 pour les actifs de type service. La figure n°42, ci-dessous présente un extrait du panorama des gravités de scénarios.

Panorama des gravités de scénarios	Disponibilité				Intégrité				Confidentialité			
	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4
<b>Actifs de type Données et informations</b>												
<i>Données et informations</i>												
D01 Fichiers de données ou bases de données applicatives	0	0	10	2	0	0	0	0	0	0	0	0
D02 Fichiers bureautiques partagés	0	0	6	0	0	0	0	0	0	0	0	0
D03 Fichiers bureautiques personnels (gérés dans environnement personnel)	0	0	0	0	0	0	0	0	0	0	0	0
D04 Informations écrites ou imprimées détenues par les utilisateurs, archives	0	0	0	0					0	0	0	0
D05 Listings ou états imprimés des applications informatiques									0	0	0	0
D06 Données échangées, écrans applicatifs, données individuellement sensibles	0	0	0	0	0	0	0	0	0	0	0	0
D07 Courrier électronique	0	0	0	0	0	0	0	0	0	0	0	0
D08 Courrier postal et télécopies	0	0	0	0	0	0	0	0	0	0	0	0
D09 Archives patrimoniales ou documentaires	0	0	0	0					0	0	0	0
D10 Archives informatiques	0	0	7	0	0	0	0	0	0	0	0	0
D11 Données et informations publiées sur des sites publics ou internes	0	0	0	0	0	0	0	0	0	0	0	0
<b>Actifs de type Services</b>												
<i>Services généraux communs</i>												
G01 Environnement de travail des utilisateurs	0	0	0	0								
G02 Services de télécommunication (voix, télécopies, visioconférence, etc.)	0	0	8	1	0	0	0	0				
<i>Services informatiques et télécom</i>												
I01 Service du réseau étendu	0	0	8	1	0	0	0	0				
I02 Service du réseau local	0	0	8	1	0	0	0	0				
S01 Services applicatifs	0	0	18	3	0	0	0	0	0	0	0	0
S02 Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	0	0	18	3	0	0	0	0				
S03 Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	0	0	0	0								
S04 Services systèmes communs : messagerie, archivage, impression, édition, etc.	0	0	0	0	0	0	0	0				
S05 Services de publication d'informations sur un site web interne ou public	0	0	0	0	0	0	0	0				

Figure n°42: Extrait du Panorama des gravités par scénarios

Le tableau des événements, offre une vue globale du nombre de scénarios par seuil de gravité, en fonction des sinistres retenus à l'issue de la cartographie des sinistres. Ainsi donc, le sinistre « dégât des eaux » serait à la base de onze (11) scénarios de niveau 4 et deux (02) scénarios de niveau 3. La figure n°43 (ci-dessous) illustre un extrait du tableau des événements.

Tableau des événements			Nombre de scénarios par niveau de gravité				
Type	Code type	Événement	Code	Gr 1	Gr 2	Gr 3	Gr 4
Absence accidentelle de personnel	AB.P	Absence de personnel de partenaire	AB.P.Pep	0	0	0	0
		Absence de personnel interne	AB.P.Per	0	0	0	0
Absence ou indisponibilité accidentelle de service	AB.S	Absence de service : Énergie	AB.S.Ene	0	0	0	0
		Absence de service : Climatisation	AB.S.Cli	0	0	0	0
		Absence de service : locaux	AB.S.Loc	0	0	0	0
		Absence de maintenance applicative ou maintenance app. impossible	AB.S.Maa	0	0	0	0
		Absence de maintenance système ou maintenance système impossible	AB.S.Mas	0	0	0	0
Accident grave d'environnement	AC.E	Foudroiement	AC.E.Fou	0	0	5	0
		Incendie	AC.E.Inc	0	0	13	0
		Inondation	AC.E.Ino	0	0	13	0
Accident matériel	AC.M	Panne d'équipement informatique ou télécom	AC.M.Equ	0	0	0	0
		Panne d'équipement de servitude	AC.M.Ser	0	0	0	0
Absence volontaire de personnel	AV.P	Conflit social avec grève	AV.P.Gre	0	0	0	0
Erreur de conception	ER.L	Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)	ER.L.Lin	0	0	0	0
Erreur matérielle ou de comportement du personnel	ER.P	Perte ou oubli de document ou de media	ER.P.Peo	0	0	0	0
		Erreur de manipulation ou dans le suivi d'une procédure	ER.P.Pro	0	0	0	0
		Erreur de saisie ou de frappe	ER.P.Prs	0	0	0	0
Incident dû à l'environnement	IC.E	Dégât dû au vieillissement	IC.E.Age	0	0	0	0
		Dégât des eaux	IC.E.De	0	0	2	11
		Surcharge électrique	IC.E.Pol	0	0	0	0
		Dégât dû à la pollution	IC.E.Se	0	0	0	0

Figure n°43: Extrait du tableau des événements

### 3.5.5. Scénarios retenus

A l'issue de la phase d'analyse, les scénarios retenus ont été recensés avec les différents niveaux de gravité à l'état actuel du système, ainsi que les différents plans possibles pour réduire, l'impact en cas d'avènement de ces scénarios.

- Perte de données applicatives
- Pertes de données bureautiques partagées
- Perte d'archives informatiques
- Indisponibilité des services de télécommunication (Voix, télécopie, visioconférence)
- Indisponibilité du service du réseau étendu (WAN)
- Indisponibilité du service du réseau local (LAN)
- Indisponibilité du service applicatif

La figure n°44 présente un aperçu des scénarios sus cités tels que présentés dans la base de connaissance Mehari.



### 3.5.6. Choix des plans d'actions

L'objectif des plans d'actions est de définir les différentes actions à entreprendre afin d'en diminuer l'impact ou d'éradiquer complètement le risque. La base de connaissance Méhari propose différents types de plans par scénarios, laissant la liberté aux équipes opérationnelles et décisionnelles d'opérer le choix qui leur convient.

On distingue les types de plans suivants:

- Type A: Plan jouant sur moins de 20 % des scénarios de la famille
- Type B: Plan jouant sur 20 % à 40 % des scénarios de la famille
- Type C: Plan jouant sur 40 % à 60 % des scénarios de la famille
- Type D: Plan jouant sur 60 % à 80 % des scénarios de la famille
- Type E: Plan jouant sur plus de 80 % des scénarios de la famille

Le choix des plans de sauvegarde a eu pour base quatre exigences fondamentales des PPM que je rappelle :

- Garantir que les informations de la société soient sauvegardées
- Eviter les pertes de données
- Garantir la disponibilité des systèmes et des traitements en cas de défaillance
- Prévoir la reprise d'activité suite à une interruption ou à un désastre

Ces exigences se traduisant bien sûr par une tolérance minimale du risque de perte de données, et l'exigence d'une continuité et une reprise rapide des activités en concordance avec les contraintes temporelles de reprise issue de l'analyse d'impact sur l'activité.

#### 3.5.6.1. Perte de données applicatives

Le choix a été porté sur l'amélioration des mesures palliatives (Plan de type E), se traduisant par:

- La sauvegarde des données applicatives
- Une sauvegarde de secours externalisé
- Une gestion rigoureuse des moyens d'accès aux données applicatives

Ce choix permettra d'éradiquer tous les scénarios de niveau de gravité 3 et 4 relatifs à cette famille de scénarios.

#### **3.5.6.2. Perte de données bureautiques partagées**

Le choix a été porté sur l'amélioration des mesures palliatives (Plan de type E), se traduisant par:

- Une sauvegarde de secours externalisé
- Une sauvegarde des données utilisateurs (bureautique) stockées sur le server de fichier.
- Une gestion rigoureuse des moyens d'accès aux fichiers bureautiques

Ce choix permettra d'éradiquer tous les scénarios de niveau 3 et 4.

#### **3.5.6.3. Perte d'archives informatiques**

Pour cette famille de scénarios, le choix a été porté sur deux plans; un plan de type B, améliorant la prévention et un plan de type D, permettant d'améliorer les mesures palliatives.

- Plan de type B:
  - Organisation de la gestion des archives informatiques
  - Gestion de la sécurité des archives
- Plan de type D
  - Gestion des accès aux archives
  - Gestion des moyens d'accès aux données applicatives

La mise en œuvre de ces mesures permettra d'isoler tous scénarios de niveau de gravité 3 ou 4.

#### **3.5.6.4. Indisponibilité des services de télécommunication**

Afin de limiter au maximum ce scénario, une mesure palliative (plan de type E) et une mesure de prévention (plan de type B) ont été adoptées.

- Plan de type E
  - Plan de reprise d'activité
  - Astreintes
- Plan de type B: Prévention des risques de dégât des eaux



#### **3.5.6.5. Indisponibilité du service de réseau étendu**

Pour limiter l'impact de cette famille de scénarios, il a été retenu l'amélioration des mesures palliatives via un plan de type E, se traduisant par la mise en œuvre d'un plan de continuité.

#### **3.5.6.6. Indisponibilité du réseau local**

La suppression des risques de gravité 3 et 4 pour cette famille de scénario, passe par un plan de type E se traduisant par :

- Plan de la maintenance des équipements du réseau local
- Procédures et plan de reprise du réseau local sur incident
- Plan de reprise d'activité du réseau local

#### **3.5.6.7. Indisponibilité de service applicatif**

Pour ce scénario, le choix a été porté sur l'amélioration des mesures palliatives, via un plan de type D, se traduisant par la mise en place d'un plan de continuité.

#### **3.5.6.8. Indisponibilité de service bureautique commun**

La suppression des risques de niveau de gravité 3 et 4 pour ce scénario a été portée par une amélioration des mesures palliatives via un plan de type A, se traduisant par une organisation des astreintes.

### 3.6. Conception de l'infrastructure optimisée

L'atteinte des objectifs de continuité d'activité tels que présentés ci-dessus, passe en premier lieu par une refonte de l'infrastructure existante intégrant une stratégie globale de continuité.

#### 3.6.1. Architecture servers

L'architecture servers qui était essentiellement constitué de servers physiques tels que présentée par la figure n°45 sera optimisée par la mise en place d'un SAN et la virtualisation des servers.

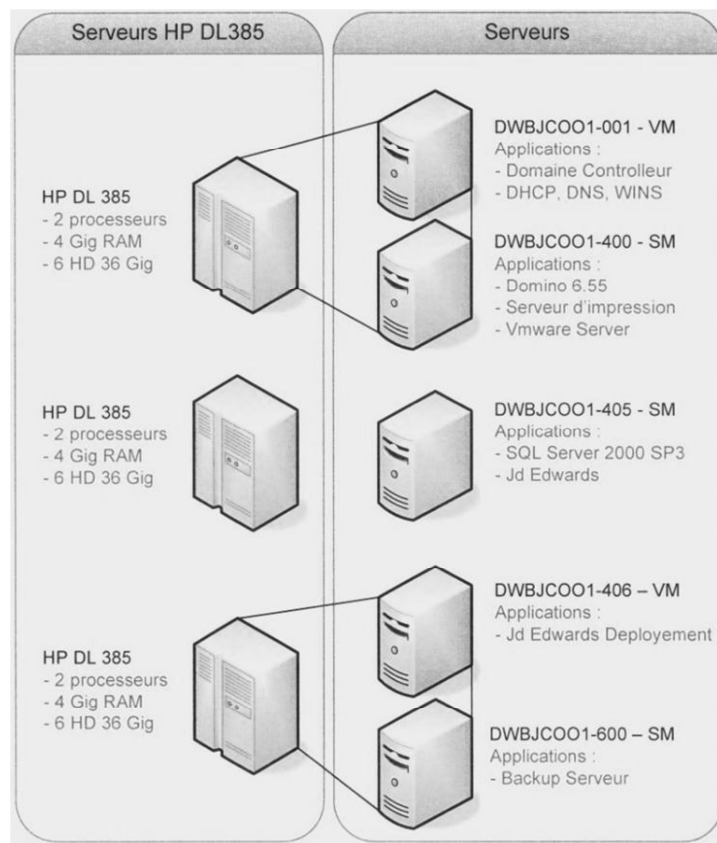


Figure n°45: Ancienne configuration servers

Il a été procédé en premier lieu à l'installation du SAN puis ensuite, la mise à jour des anciens servers fonctionnant sous l'OS Windows 2003, vers le nouveau système d'exploitation (Windows 2008 Enterprise servers R2), via la virtualisation des machines. Cette stratégie a également l'avantage de permettre une réduction conséquente du temps de reprise en cas de sinistre.

En ce qui concerne les solutions techniques, notre choix s'est porté sur la technologie SAN de EMC, qui permet d'obtenir un haut niveau de sécurité, une gestion aisée, une augmentation à volonté des ressources de stockage et une redondance des périphériques. La virtualisation quant à elle, sera assurée avec VMWARE qui apporte une meilleure optimisation des ressources, une haute disponibilité et un déploiement aisé des machines virtuelles.

### **3.6.2. Infrastructure de sauvegarde**

La stratégie de sauvegarde et de restauration a été repensée. Le nouveau robot de sauvegarde permettra de sauvegarder des données à hauteur du téraoctet (To). Les règles de sauvegarde intègrent à la fois la sauvegarde incrémentale sur disque, la sauvegarde complète et une duplication sur bande qui sera externalisée. Le Logiciel Symantec Backup Exec 2010, précédemment utilisé sera remplacé par sa version 2012, qui permet la correction des bugs liés au composant AOF et enfin, le précédent serveur de sauvegarde (HP DL385) ne supportant pas la nouvelle version prévue du système d'exploitation, sera remplacé par un nouveau.

### **3.6.3. Réplication inter sites**

La technologie Falconstor permettra l'usage du système de déduplication des données (réduction de la taille des données), la réplication vers un site secondaire et une reprise rapide. La programmation de la réplication de données entre les deux sites est de 2 heures. En d'autres termes, nous pouvons perdre un maximum de 2 heures de données en cas de désastre.

## **3.7. Implémentation des solutions techniques**

Nous présentons dans ce sous chapitre les différentes solutions techniques adoptées et ou implémentées suite à la phase de définition des stratégies.

### **3.7.1. Servers**

Outre la virtualisation, il sera dédié deux nouveaux serveurs physiques, qui assureront respectivement le rôle de serveur d'archives informatiques et de serveur de fichiers. Ci-dessous un aperçu comparatif des deux panoramas de serveurs (serveurs en fin de vie versus nouvelles machines virtuelles).

## Panorama des Servers en fin de vie

DWBJCOO1-400	172.18.26.21	→	Server de messagerie (Lotus) / Server de fichier
DWBJCOO1-401	172.18.26.23	→	Server de déploiement (ERP JDE)
DWBJCOO1-402	172.18.26.24	→	Server de production (ERP JDE)
DWBJCOO1-403	172.18.26.27	→	Terminal Server
DWBJCOO1-201	172.18.26.25	→	Server d'impression et d'antivirus (McAfee)
DWBJCOO1-001	172.18.26.20	→	Server d'active directory
DWBJCOO1-600	172.18.26.22	→	Server de backup

VS

## Panorama des nouvelles machines virtuelles

DWBJCOO1-400	172.18.26.21	→	Server de messagerie (Lotus Domino)
DWBJCOO1-410	172.18.26.207	→	Server de déploiement (ERP JDE)
DWBJCOO1-411	172.18.26.208	→	Server de production (ERP JDE)
DWBJCOO1-412	172.18.26.209	→	Server WEB JDE
DWBJCOO1-415	172.18.26.211	→	Server de fichier
DWBJCOO1-202	172.18.26.206	→	Server d'impression et d'antivirus (McAfee)
DWBJCOO1-005	172.18.26.10	→	Server d'active directory
DWBJCOO1-409	172.18.26.213	→	Server d'archivage Lotus Notes
DWBJCOO1-VC001	172.18.26.205	→	Vcenter 4.1

### 3.7.2. Virtualisation

#### 3.7.2.1. Virtual Center

VMware Virtual center fournit une gestion centralisée, une automatisation des opérations, une optimisation des ressources, et une haute disponibilité pour les environnements informatiques. La virtualisation est basée sur les services distribués afin d'équiper le data center avec des niveaux sans précédent de réactivité et une facilité d'entretien, l'efficacité et la fiabilité. Virtual center offre un haut niveau de simplicité et d'efficacité, la sécurité et l'efficacité nécessaire pour gérer un environnement informatique virtualisé de n'importe quelle taille. On distingue :

- Le VirtualCenter Server, qui est le nœud de commande principal pour gérer l'environnement IT, la Base de données VirtualCenter, qui facilite le stockage à long terme des données et des ressources virtuelles.

- Le VirtualCenter client, qui facilite les connexions d'utilisateurs distants au Server ESX ou au VirtualCenter Server
- Le VirtualCenter Agent, qui facilite la communication entre le server ESX et le VirtualCenter Server,
- Le VirtualCenter Web Access, qui facilite la gestion de machine virtuelle sans l'installation d'un client.

La figure n°46, ci-dessous illustre le positionnement du « VirtualCenter ».

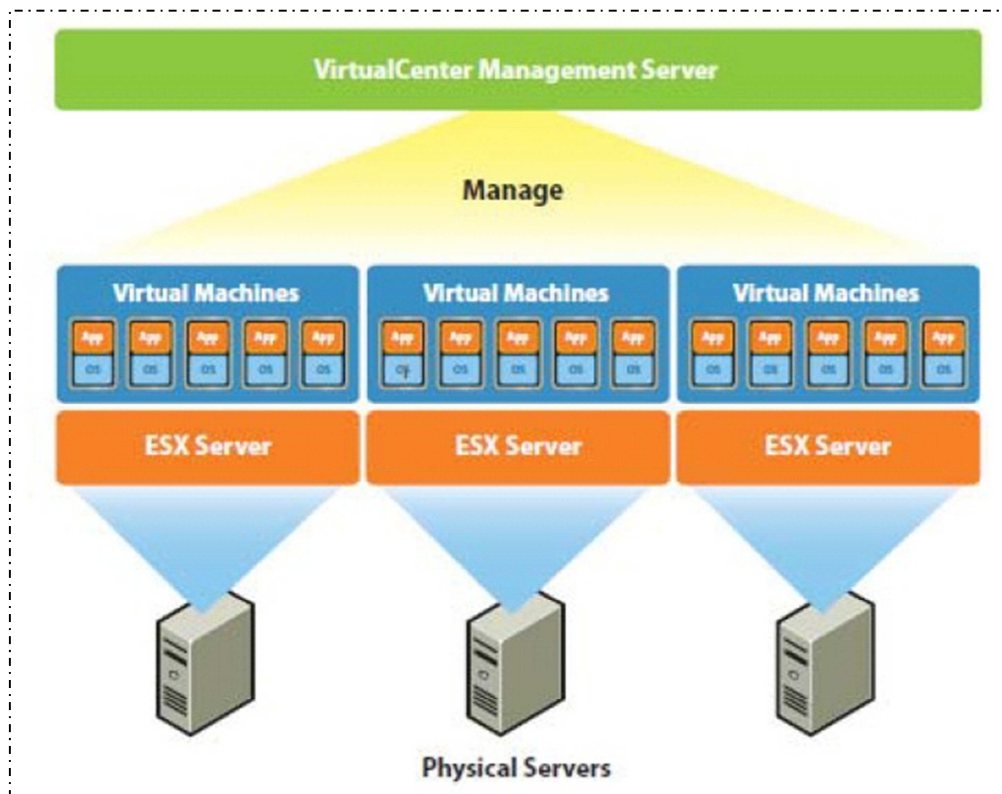


Figure n°46: Positionnement du Virtual Center

### 3.7.2.2. Gestion des servers ESX

La gestion des deux servers ESX est assurée via l'interface VMware client. Comme l'illustre la figure n°47, la connexion du client au DWBJCOO1-VC001, qui est le centre virtuel donne l'accès au management des servers ESX.

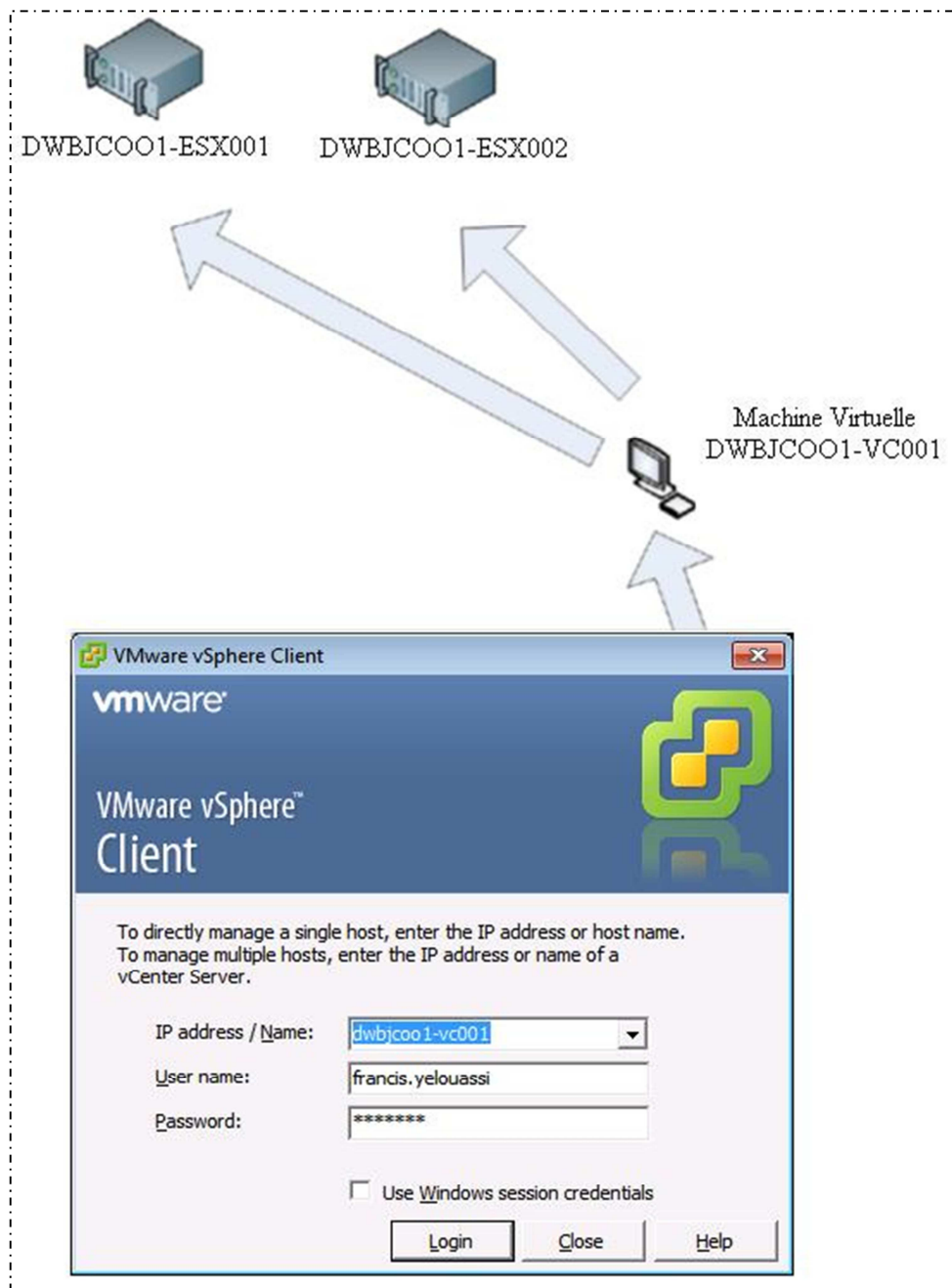


Figure n°47: Gestion ESX

### 3.7.3. Configuration SAN

Le SAN choisit est de la marque EMC2. Il s'agit en fait d'une VNXe3100. L'installation s'est effectuée avec l'appui du DRP Administrator. L'interconnexion des processeurs de stockage au réseau informatique d'OBSA a été assurée par un câblage de la catégorie 5e (CAT5e) et le branchement électrique des DPE par deux sources de tension électriques indépendantes. La figure n°48 ci-dessous, donne un aperçu de

l'environnement virtualisé suite à l'installation du SAN et de la virtualisation des servers. On voit bien les deux servers ESX et les machines virtuelles.

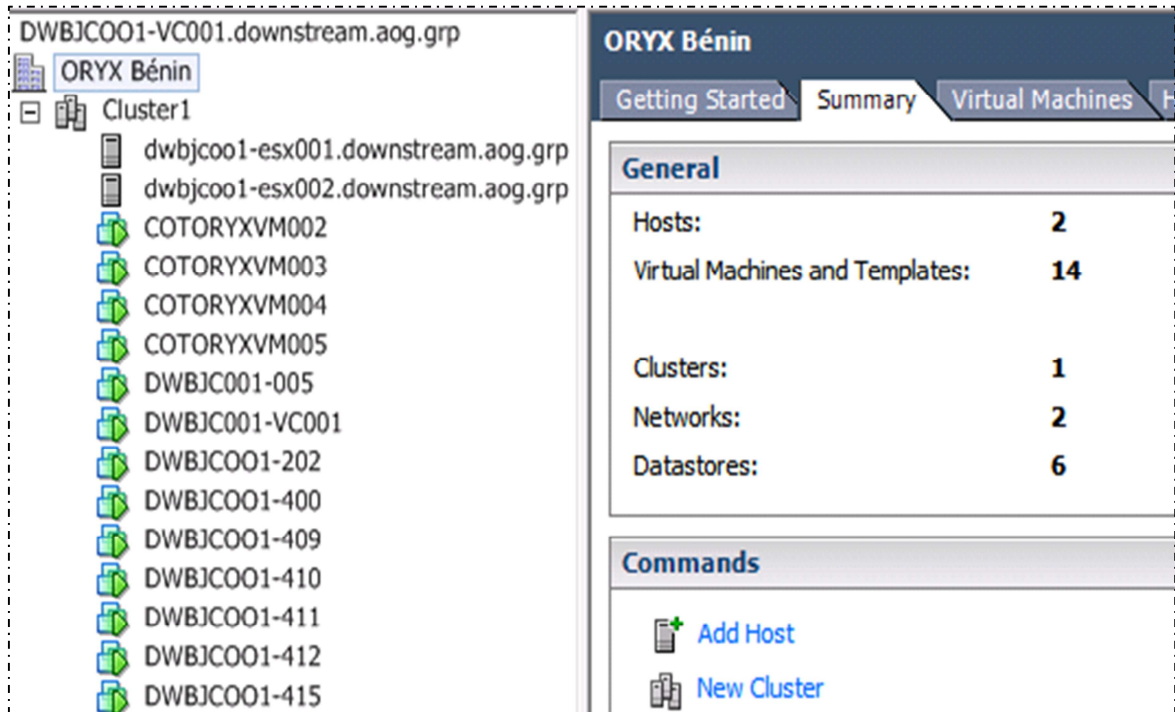


Figure n°48: Aperçu VM

Les machines virtuelles sont réparties entre les servers ESX. La figure n°49 ci-dessous présente les machines virtuelles suivant leur rattachement.

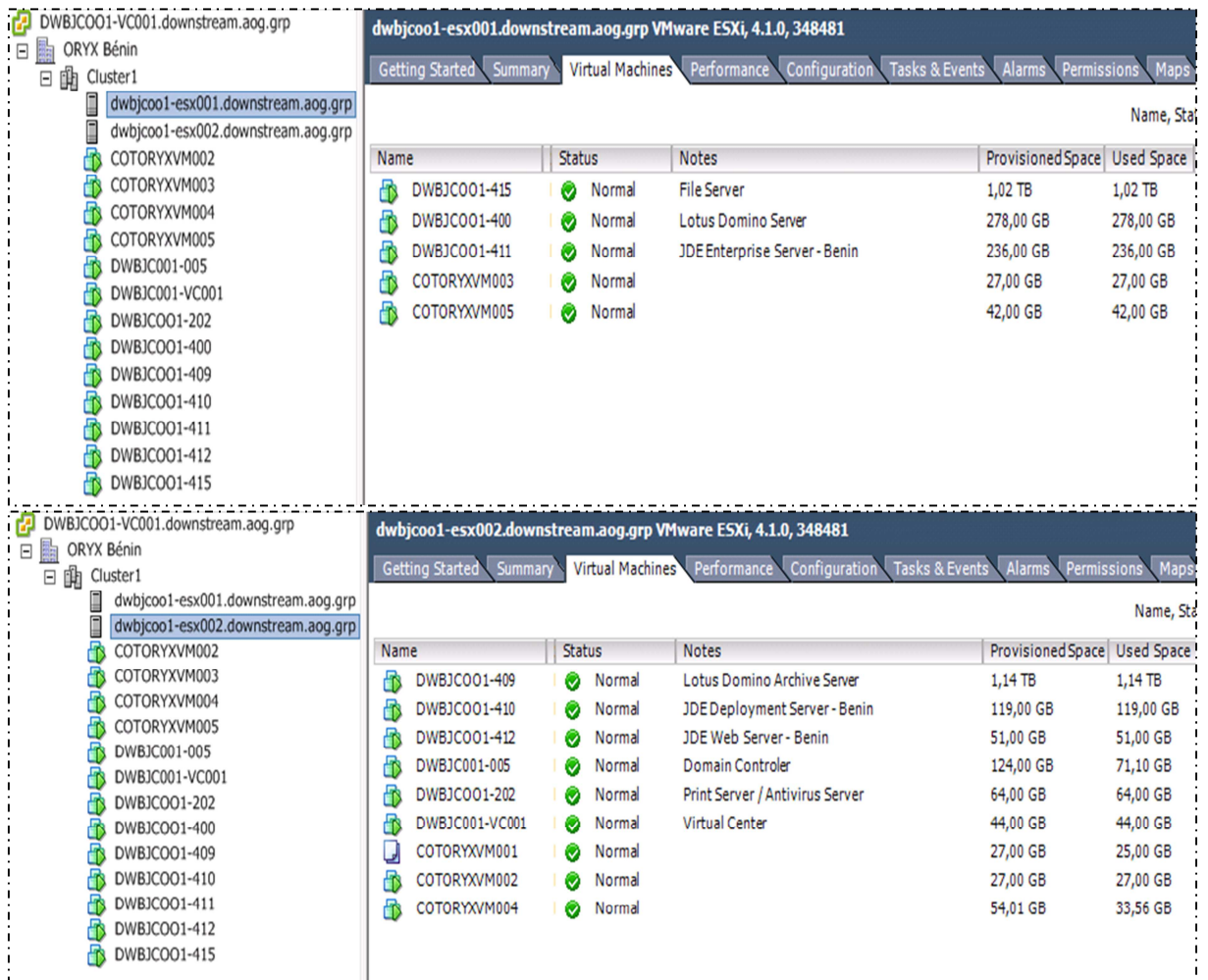


Figure n°49: Répartition des VM

### 3.7.4. LUN – Zoning – Masking

Chaque serveur voit l'espace disque de la baie SAN auquel il a accès comme son propre disque dur. Il a donc été défini tel que recommandé par les bonnes pratiques, les « Logical unit number » (LUN, unités logiques), le masking et le zoning, afin d'éviter par exemple qu'un serveur Unix n'accède aux mêmes ressources qu'un serveur Windows utilisant un système de fichier différent. Ci-dessous, les figures n°50 et n°51 présentent, les LUN tels que définis dans le cadre de la refonte du SI d'OBSA.



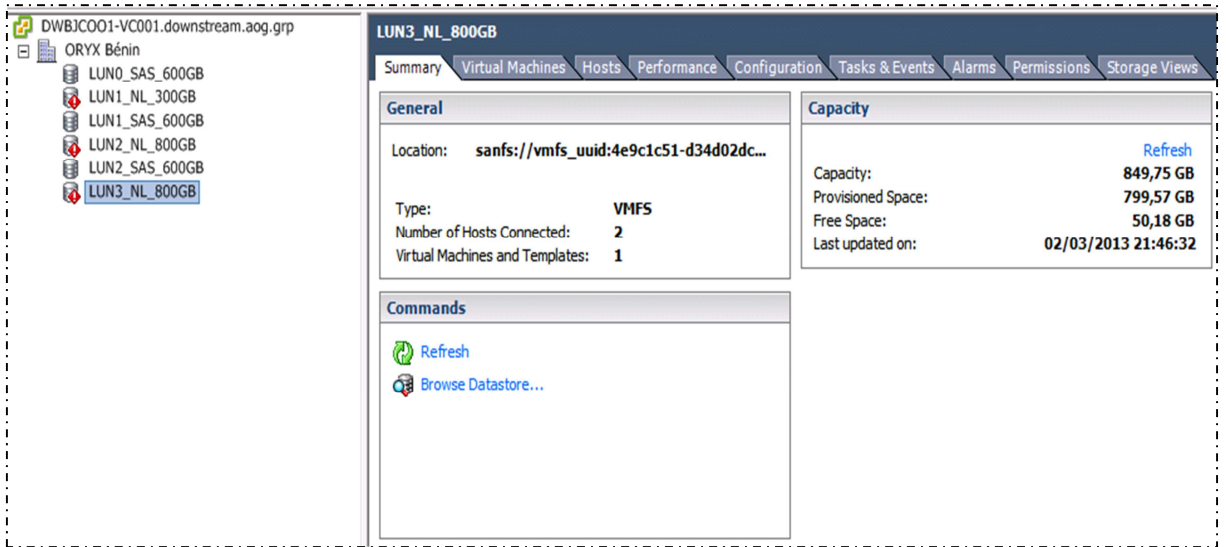


Figure n°50: LUN - SAN

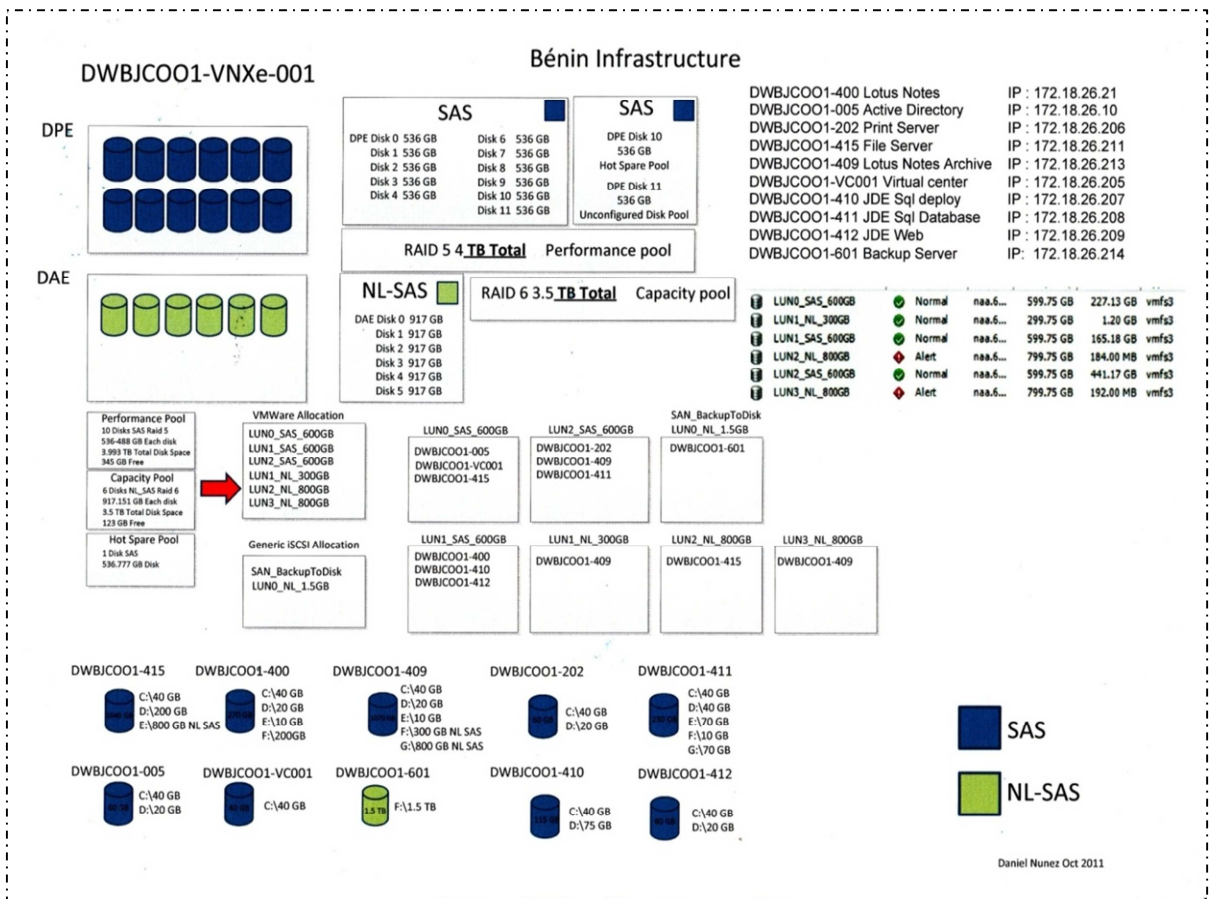


Figure n°51: LUN - Répartition

### 3.7.5. Infrastructure de sauvegarde

La nouvelle infrastructure de sauvegarde est constituée comme suit:

- Un server HP ML 380
- Un lecteur LTO4 + 40 tapes SDLT (1,2 To)
- Logiciel: Symantec Backup exec 2012

La stratégie de sauvegarde retenue se traduit par une sauvegarde quotidienne incrémentale sur disque, du lundi au vendredi et une sauvegarde complète tous les samedis. Dès la fin de la sauvegarde complète, se déclenche le processus de duplication qui consiste à transférer la sauvegarde complète ainsi réalisée sur une tape.

La figure n°52 (ci-dessous) donne un aperçu des trois jobs de sauvegarde telle que programmés via le logiciel Symantec Backup exec 2012.

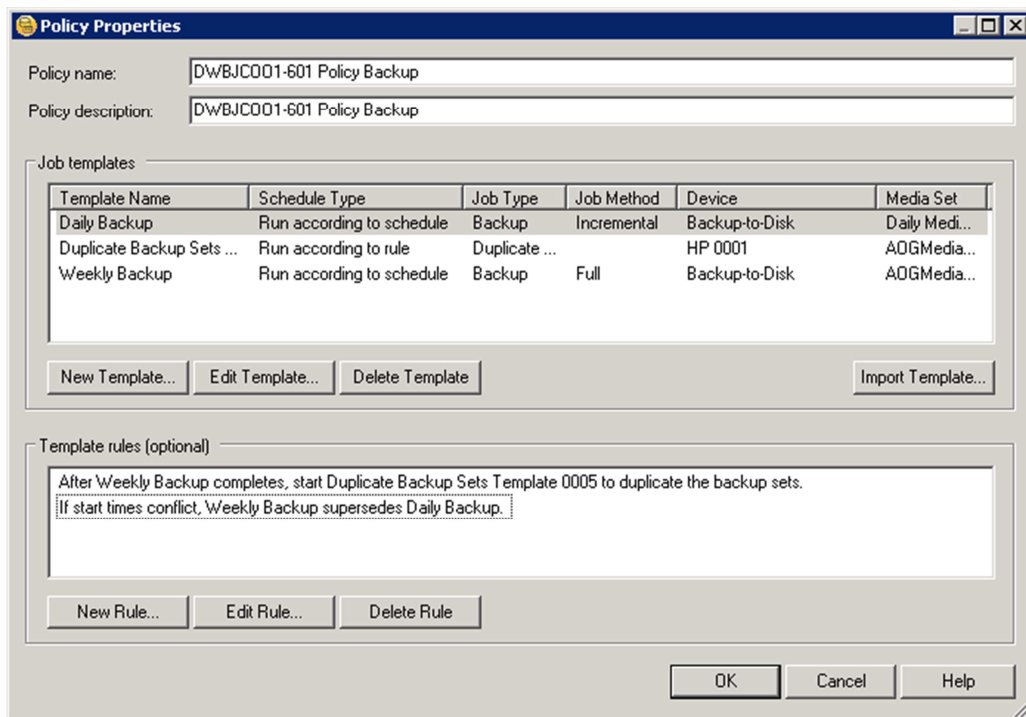


Figure n°52: Ecran «job setup»

Le comportement attendu du système en cas de conflit entre job de sauvegarde, d'échec d'un job précédant, l'ordre d'exécution des jobs...etc., se traduit par des règles de gestion des templates. La figure n°53 présente les règles de gestion des templates tel que programmés chez OBSA.

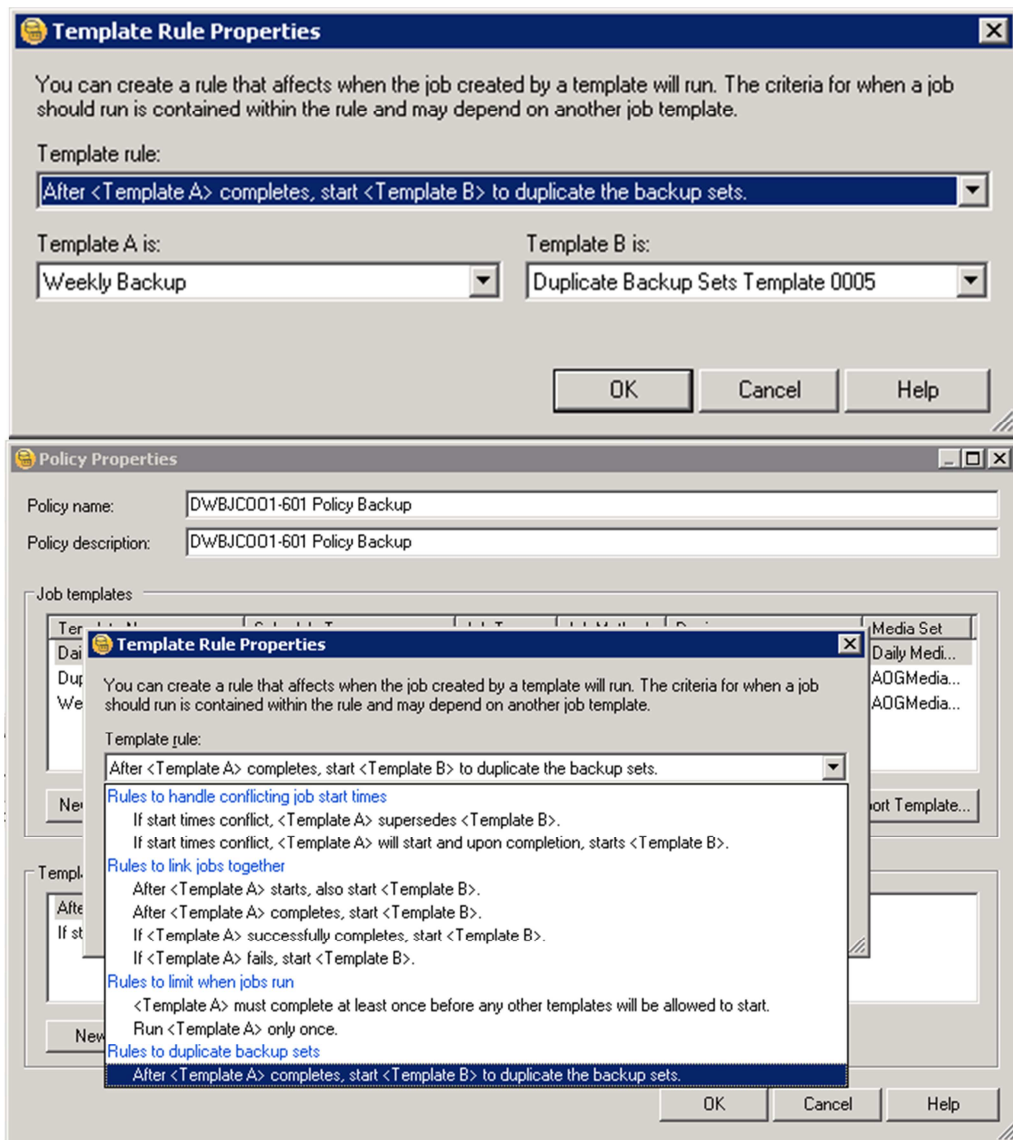


Figure n°53: Règles de Template

La liste de sauvegarde intègre toutes les données sauvegardées, qui sont essentiellement constituées des données utilisateurs sauvegardées sur les servers, les bases de données applicatives, les applications et licence, les bases de document Lotus Notes, les machines virtuelles et les archives informatiques. La figure n°54, ci-dessous donne un aperçu de la liste de sauvegarde.

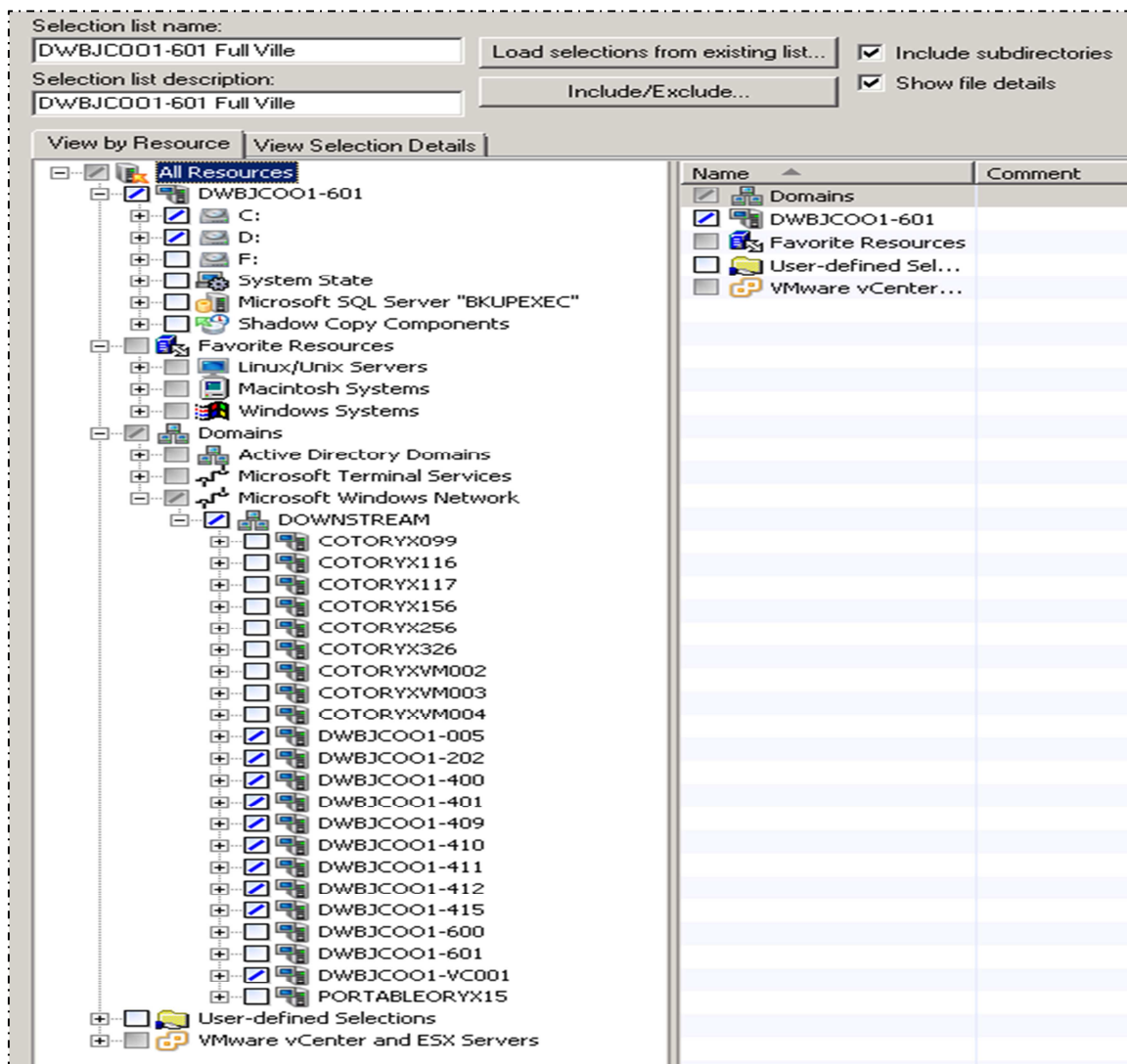


Figure n°54: Liste de sauvegarde

Il a été mise en place, à cette occasion, des règles strictes en matière de gestion de la sauvegarde des données. Ainsi, un coffre a été loué à la banque pour l'externalisation des sauvegardes (via duplication) sur tapes. Ci-dessous (Figure n°55) un aperçu de la communication du DRP Administrator à cet effet. La figure n°56, illustre l'algorithme de la nouvelle procédure de sauvegarde telle qu'appliquée chez OBSA.

Dear colleagues,

Meanwhile installing the local DRP on your site, we have to complete the local backup strategy following those procedures :

After the backup, the designed operator must verify the success of the operation (read logs on system).

All sites must physically move daily backup tapes to an external site.

A person will be responsible to give the last backup tapes to the messenger. Another person will be designated to receipt tapes and safe them on the external site.

For security reasons, we suggest to keep the last two daily backups on the secondary site.

Daniel NUNEZ

Disaster Recovery Plan Group Administrator

Figure n°55: Extrait de note de service

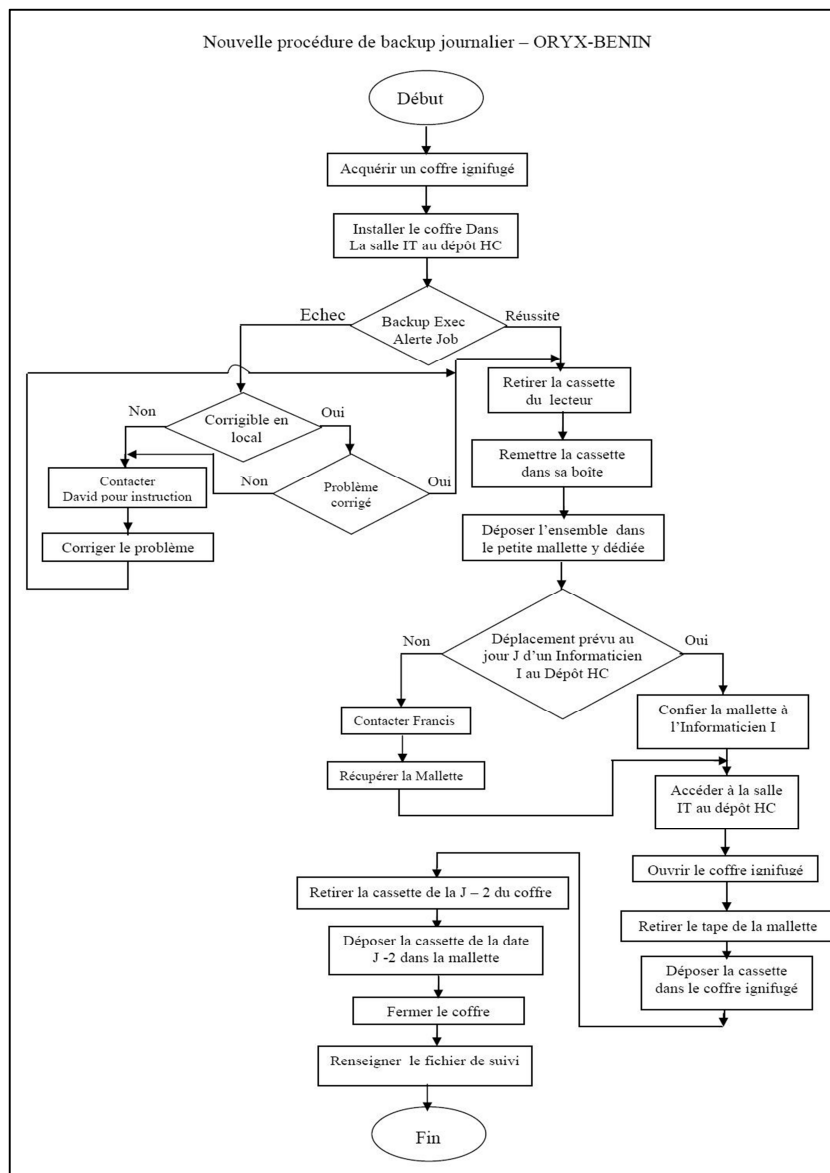


Figure n°56: Algorithme Gestion du backup

### 3.7.6. Topologie après refonte

La figure n°57 (ci-dessous), présente la topologie du réseau d'OBSA après la refonte.

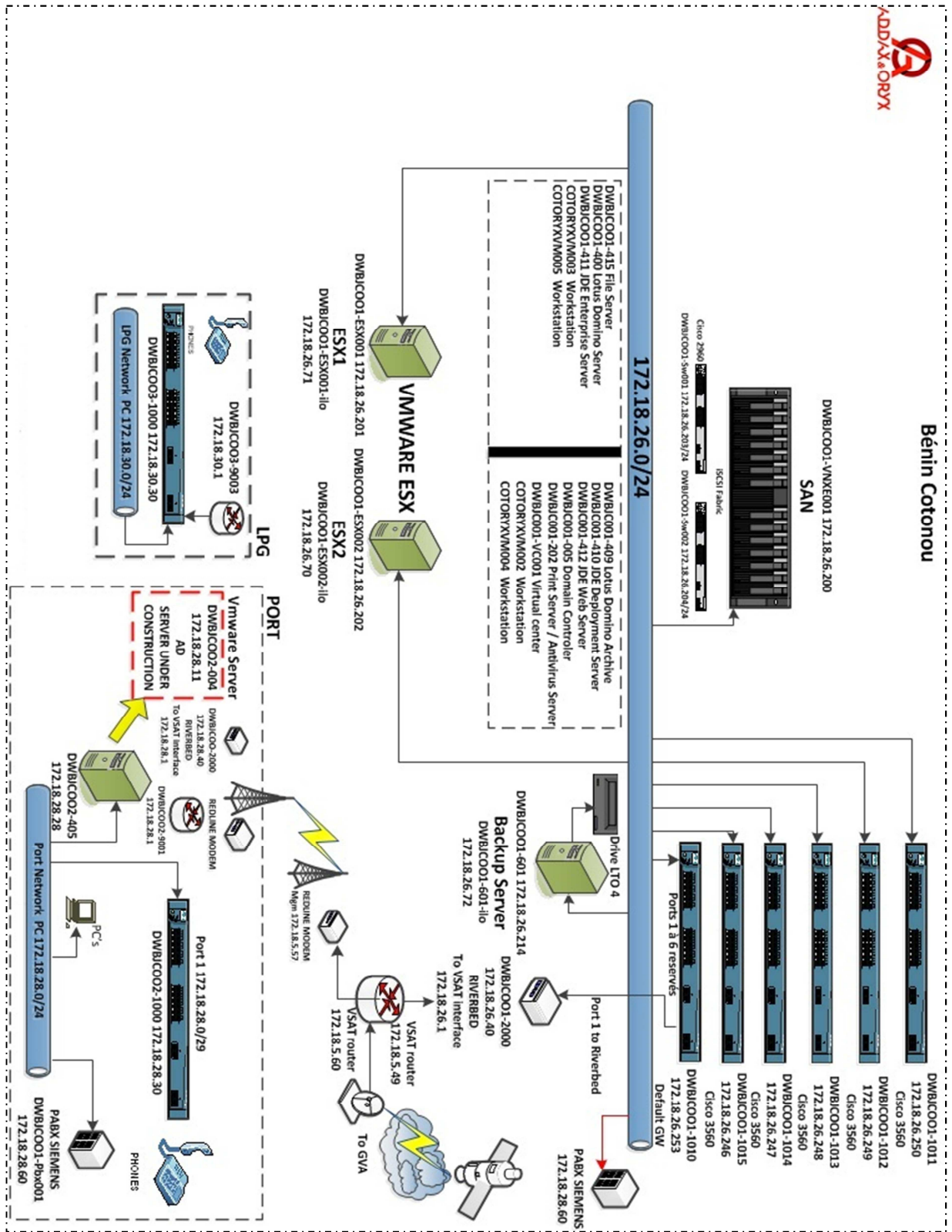


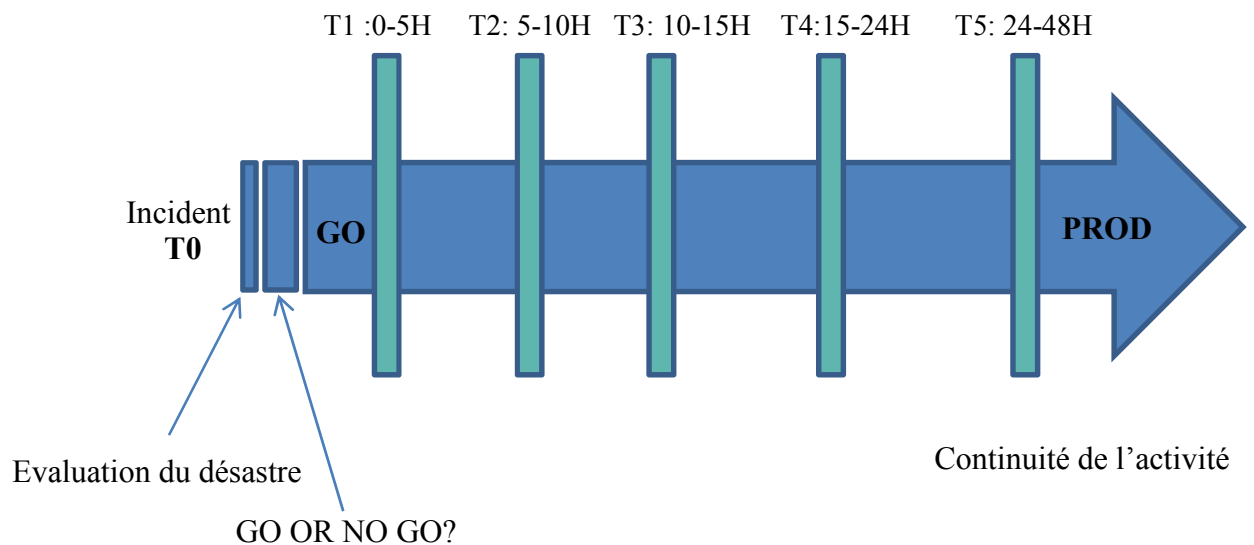
Figure n°57: Topologie après refonte

### 3.7.7. Réplication inter sites

Les objectifs en temps de reprise admis par le comité de pilotage sont les suivants:

- Le RTO a été fixé à 48H
- Le RPO a été fixé à 24H

Ci-dessous, illustrées, les différentes phases devant marquer le déclenchement du plan de continuité.



Ci-dessous, les détails des opérations à effectuer durant chaque laps de temps

- T0: La salle de replie est prête
- T1: Activation et basculent réseau de l'infrastructure DRP
- T2: Test des servers et des données
- T3: Activation et vérification des équipements informatiques de la salle de repli
- T4: Vérification de l'infrastructure de télécommunication
- T5: Déplacer les utilisateurs vers la salle de repli

La stratégie adoptée consiste à exploiter la salle informatique du dépôt comme salle de repli. Cette salle sera équipée d'un SAN, et de toute l'infrastructure applicative et matériel permettant aux utilisateurs critiques en cas de crise, d'accéder au système du dépôt et travailler avec un delta données maximum de deux heures. La mise à jour des données critiques étant assurée par une réplication entre le site de la Direction et le site

du Dépôt via la liaison microwave. La figures n°58 illustre l'infrastructure DRP tel que conçue.

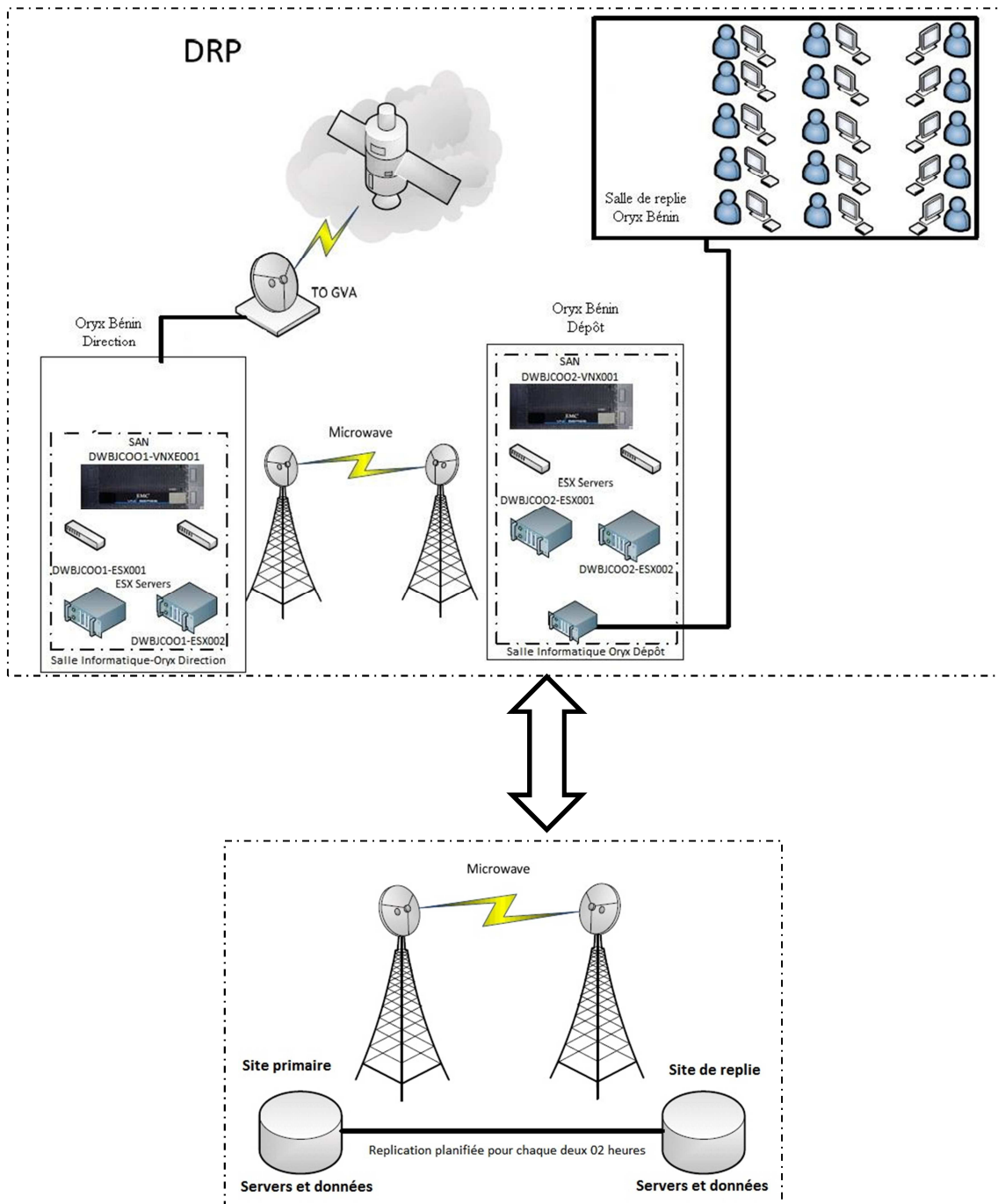


Figure n°58: Infrastructure DRP

Tous les utilisateurs installés dans la salle de repli pourront accéder à toutes les ressources et aux fichiers en utilisant leur login (Couple nom d'utilisateur et mot de passe) tel qu'illustré par la figure n°59, ci-dessous.





Figure n°59: Login utilisateur

### 3.7.7.1. Stratégie Falconstor et configuration

Tous les disques durs VM (machine virtuelle) sont répliqués dans l'appliance CDP (Clean Desk Policy) du site LIVE en mode continu. L'Appliance CDP est configuré pour créer une copie instantanée chaque heure avec un maximum de 48 h en mode FIFO. La réplication entre le site CDP LIVE et le site du CDP DRP se produit toutes les deux heures. La figure n°60, ci-dessous, illustre le processus ci-dessus présenté.

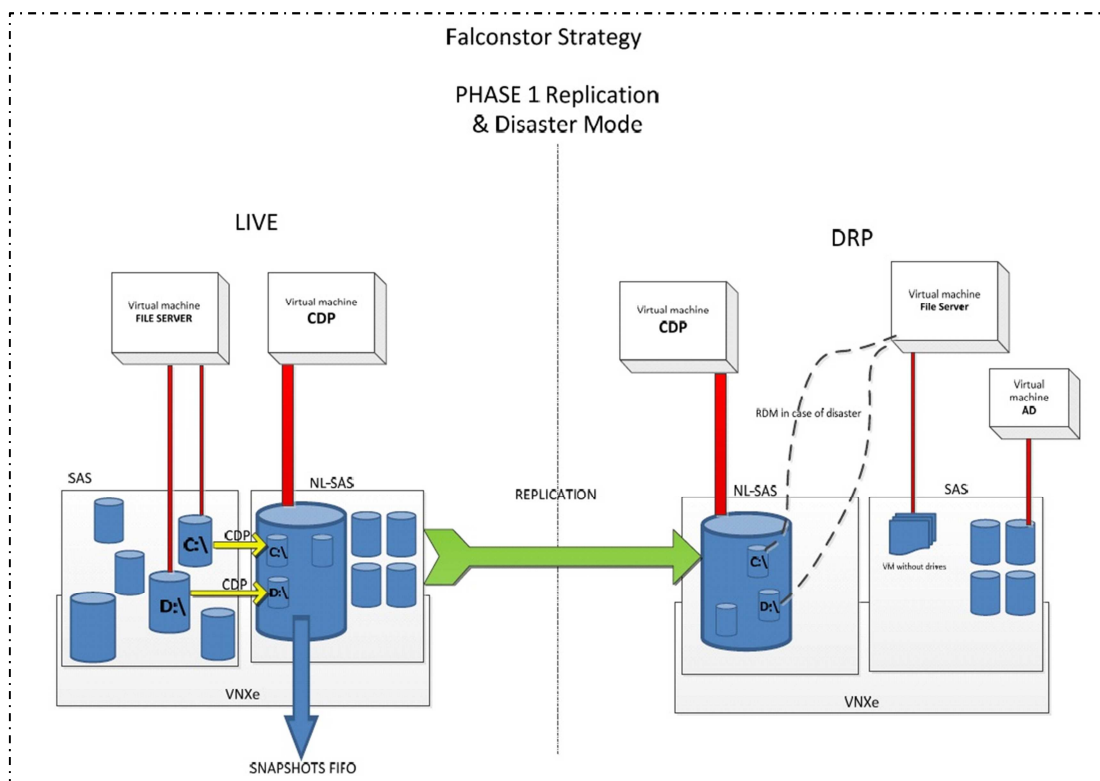


Figure n°60: Stratégie Falconstor

### 3.7.7.2. Etat de basculement

En cas de basculement du site LIVE, le CDP charge les pilotes via RDM (Raw Device Mapping) pour les machines virtuelles existantes. Les utilisateurs peuvent alors se connecter aux machines virtuelles et continuer à travailler. Le delta données peut aller jusqu'à deux heures (au sens de la réplication entre site). Dans ce cas, les réseaux et sous réseaux peuvent éventuellement changer. La figure n°61 ci-dessous illustre le principe de l'état de basculement.

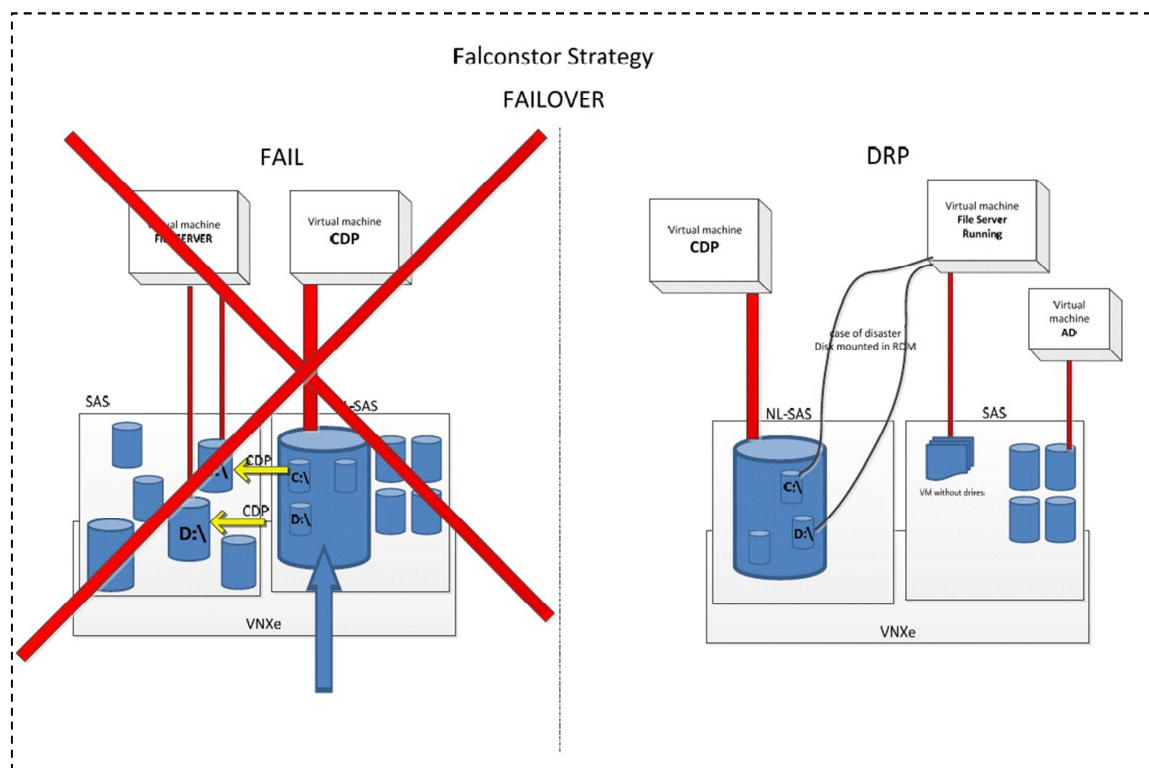


Figure n°61: Etat de basculement

### 3.7.7.3. Retour à la normale

Lorsque le site principal (LIVE) redevient disponible, il convient de procéder à la réplication des données du CDP DRP vers le CDP LIVE, restaurer les machines virtuelles et synchroniser les disques depuis le LUN du CDP vers les disques de la VM originale. La figure n°62 ci-dessous illustre le retour à la normale.

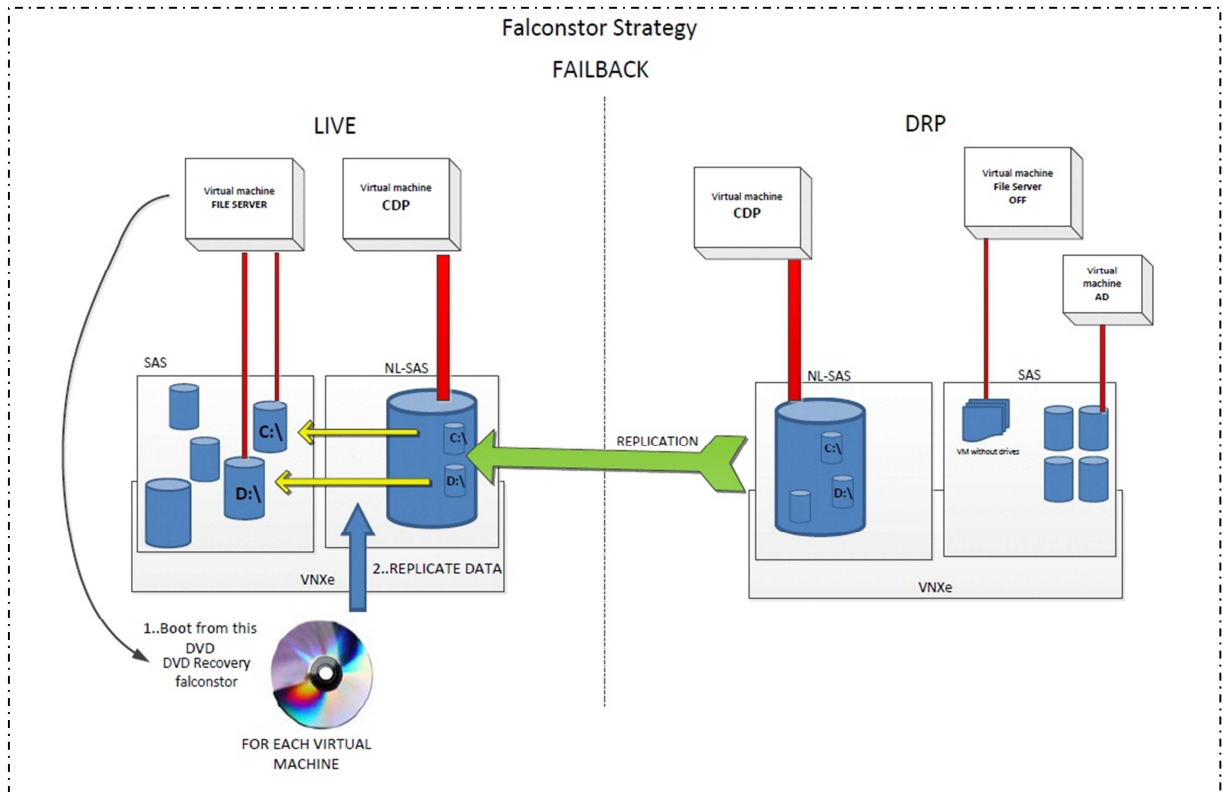


Figure n°62: Retour à la normale

## **3.8. Elaboration des plans et procédures de continuité**

### **3.8.1. Maintenance DRP**

Chaque année, il est prévu d'organiser une rencontre administrative et technique pour discuter des changements ayant survenus au cours de l'année et les changements prévus au sein de l'organisation. Les impacts seront évalués et suivant la validation du management, les améliorations en termes de DRP & BCP administratives, organisationnels, plans d'actions, évaluation de risque et d'architectures techniques seront implémentées.

### **3.8.2. Tests**

Tous les processus techniques implémentés ont été testés et validés. Il est prévu un test par an durant le weekend. Le prochain test est prévu pour l'année 2014.

### **3.8.3. Plan de gestion de crise**

Ce document décrit l'ensemble des acteurs et leurs responsabilités. Il comprend les étapes de la gestion de crise, de la survenance du sinistre à la reprise d'activité. Ce plan contient en annexe, les fiches réflexes d'analyse d'incidents, le tableau de bord de contrôle des sauvegardes et les règles générales relatives aux cassettes de sauvegarde, également annexées au présent mémoire.

### **3.8.4. Procédure de sauvegarde**

Ce document décrit les processus de sauvegarde mis en œuvre pour assurer les sauvegardes des données. Il contient également les procédures de restauration de chaque type de données sauvegardées.

### **3.8.5. Plan de continuité et de reprise informatique**

Ce document décrit l'architecture informatique d'OBSA. Il décrit également les mesures techniques de secours mises en œuvre pour assurer la continuité informatique des applications métiers. Ce plan contient en annexe, les fiches réflexes d'analyse d'incidents, présentées en annexe de ce mémoire.

### **3.9. Retour d'expérience**

#### **3.9.1. Préambule**

Suite à la refonte de l'infrastructure informatique d'OBSA dans le cadre du projet DRP, divers incidents ont permis de jauger le plan de continuité informatique. Les différentes réponses apportées à ces incidents ont données lieu à un retour d'expérience qui sera présenté dans ce chapitre.

Il importe de noter que le retour d'expérience qui est un processus structuré, pratiqué à l'occasion d'accident, de situation d'urgence ou d'écart constaté par rapport à la norme ou au fonctionnement normal d'une organisation, constitue un outil d'apprentissage pour cette dernière et contribue ainsi à optimiser sur les plans humains, organisationnels et techniques. Deux éléments majeurs déterminent le niveau et implicitement, l'opportunité de la conduite d'un retour d'expérience :

- Le niveau de perturbation de l'organisation
- Le potentiel d'apprentissage de la gestion de l'évènement

L'échelle de gravité graduée en fonction du niveau de perturbation des activités permet d'évaluer cette dernière, tandis que l'évaluation du potentiel d'apprentissage quant - à elle, est du ressort du comité de pilotage.

Je présente dans le cadre de ce mémoire, les retours d'expérience relatifs aux situations suivantes:

- Perte de la carte LLC du module d'extension de la baie SAN.
- Panne de l'antenne radio Redline assurant la liaison entre la Direction et le dépôt pétrolier et gazier du Bénin.
- Suppression accidentelle de données critiques par un utilisateur au Bénin.
- Panne de la liaison VSAT.

#### **3.9.2. Fiches de synthèses**

Les RETEX (retour d'expérience) seront présentés sous forme de fiches synthétiques, mettant en évidence pour chaque évènement, les faits, la solution apportée, la problématique soulevée, les axes d'amélioration et le plan d'action.

➤ **Perte de la carte LLC du module d'extension de la baie SAN**

INFORMATION GENERALE	
Date: 15/05/2013	Site: Direction Générale
Durée: 10 jours	Pays: Bénin
<b>Intitulé:</b> Perte d'une des cartes LLC du module d'extension de la baie SAN	
Gestion opérationnelle <input checked="" type="checkbox"/> Exercice <input type="checkbox"/> Autres <input type="checkbox"/>	
Auteurs: Francis YELOUASSI	
DESCRIPTIF DE L'EVENEMENT	
<p><b>Description:</b> Envoie intempestifs de l'alerte suivante par le système</p> <div style="background-color: #f0f0f0; padding: 10px;"> <p><b>CRITICAL message from VNXe (DWBJCOO1-VNXE001/172.18.26.200)</b></p> <p>You have received this email alert because an event has occurred on your VNXe (DWBJCOO1VNXE001/172.18.26.200) system of which you need to be aware and take action to correct. The alert is: System DWBJCOO1-VNXE001 has experienced one or more problems that have left it in a non-recoverable state. To learn more about this alert, open Unisphere and click Monitor → System Alerts and then click on the alert. You may also want to go to the System Health page (Monitor → System Health) to further investigate the situation.</p> <p style="text-align: center;">Message ID: 14:60518</p> </div> <p>Un ingénieur EMC2 a été sollicité pour l'analyse de la situation. Il s'est avéré qu'il s'agissait de la panne d'une des cartes LLC de la baie de stockage SAN.</p> <p>Nous étions en plein processus de transfert de données des machines physiques vers les machines virtuelles.</p> <p>Il a fallu attendre les conclusions de l'ingénieur EMC2 et commander la carte défaillante, qui nous parviendra plus d'une semaine après.</p>	
<b>Conséquences:</b> Risque d'indisponibilité totale des machines virtuelles entraînant le blocage de la migration.	
<b>Solution:</b> Remplacement systématique et sans délai de la carte LLC défaillante.	
<b>Acteurs impliqués:</b> Francis Yelouassi, Daniel NUNEZ	
PROBLEMATIQUE SOULEVEES	
Anticipation	
AXES D'AMELIORATION	
<ul style="list-style-type: none"> <li>• Prise en main des systèmes.</li> <li>• Connaissance du niveau de perte des ressources critiques.</li> </ul>	

PLAN D'ACTION			
Action à entreprendre	Service en charge de l'action	Echéancier	Observations
Inventorier et disposer d'une réserve de pièces de rechanges.	Informatique	Juin 2013	Former les ressources locales à une prise en main de premier niveau.

- **Panne de l'antenne radio assurant la liaison entre le site de la direction et le dépôt pétrolier et gazier.**

INFORMATION GENERALE	
Date: 01 juillet 2013	Site: Direction General
Durée: ½ journée	Pays: Benin
Intitulé: Panne de la liaison BLR (boucle locale radio)	
Gestion opérationnelle <input checked="" type="checkbox"/> Exercice <input type="checkbox"/> Autres <input type="checkbox"/>	
Auteur: Francis Yelouassi	
DESCRIPTIF DE L'EVENEMENT	
<p><b>Description:</b> Suite aux plaintes des utilisateurs des dépôts hydrocarbures et GPL par rapport à l'indisponibilité des services ERP, mail et des appels téléphoniques vers la Direction Générale. Une analyse de la situation par le service IT a révélé une panne au niveau du MODEM de l'antenne Redline assurant la liaison entre les deux sites.</p>	
<p><b>Conséquences:</b></p> <ul style="list-style-type: none"> <li>• Les utilisateurs des dépôts GPL et HC ne peuvent plus se connecter aux applications de messagerie et à l'ERP situé à la Direction Générale.</li> <li>• Impossibilité d'échanger des appels téléphoniques entre les deux sites</li> <li>• Blocage total des activités de chargement et de libération des camions</li> </ul>	
<p><b>Solution:</b> Basculement vers une antenne de secours, le temps d'analyser les causes et remettre en état de fonctionnement, l'antenne en panne. Il a fallu connecter la nouvelle antenne et solliciter un prestataire externe pour la configuration du modem.</p> <p>Cette solution de secours a permis la relance du service de transfert de données, mais</p>	

pas la téléphonie.			
<b>Acteurs impliqués:</b> Francis Yelouassi – Chabi Gani Alidou			
PROBLEMATIQUE SOULEVEES			
Périmètre du plan de continuité			
AXES DE PROGRES			
Amélioration de la résilience des moyens de transmissions.			
PLAN D'ACTION			
Action à entreprendre	Service en charge de l'action	Echéancier	Observations
Implémenter un système de « load balancing » de la boucle locale radio intégrant le secours de la téléphonie	Informatique	Septembre 2013	RAS

➤ **Suppression accidentelle de données critiques**

INFORMATION GENERALE	
Date: 10/04/2013	Site: Direction Générale
Durée: ½ journée	Pays: Bénin
<b>Intitulé:</b> Perte de données critiques	
Gestion opérationnelle <input checked="" type="checkbox"/> Exercice <input type="checkbox"/> Autres <input type="checkbox"/>	
<b>Auteur:</b> Francis Yelouassi	
DESCRIPTIF DE L'EVENEMENT	
<b>Description:</b> Le responsable des ressources humaines supprime par inadvertance la bibliothèque contractuelle qui représente la base de données des contrats liant la société. Il fait appel au service informatique pour l'aider à récupérer ces données.	
<b>Conséquences:</b> Impossible d'accéder aux versions numériques des contrats entraînant des fouilles intempestives aux archives et implicitement une perte de temps.	
<b>Solution:</b> Restaurer les informations sauvegardées la veille, via Veritas Backup Exec.	
<b>Acteurs impliqués:</b> Francis Yelouassi	
PROBLEMATIQUE SOULEVEES	
<ul style="list-style-type: none"> <li>• Problématique du delta donnée.</li> <li>• Sécurité physique des données</li> </ul>	
AXES DE PROGRES	



Dématérialisation des données de la bibliothèque contractuelle.			
PLAN D'ACTION			
Action à entreprendre	Service en charge de l'action	Echéancier	Observations
Mettre en place l'infrastructure de réplication des données et implémenter un logiciel de GED	Service Informatique		Associer les utilisateurs

➤ **Panne de la liaison VSAT**

INFORMATION GENERALE			
Date: 04/06/2013	Site: Direction Générale		
Durée: 01 jour	Pays: Bénin		
Intitulé: Panne de la liaison VSAT			
Gestion opérationnelle <input checked="" type="checkbox"/> Exercice <input type="checkbox"/> Autres <input type="checkbox"/>			
Auteur:			
DESCRIPTIF DE L'EVENEMENT			
<b>Description:</b> Indisponibilité de la connexion internet pour des raisons de maintenance chez le prestataire.			
<b>Conséquences:</b>			
<ul style="list-style-type: none"> <li>• Impossible d'accéder à internet et aux appels par satellite.</li> <li>• Impossible de recevoir et d'envoyer des messages à l'extérieur.</li> </ul>			
<b>Solution:</b> Activation manuelle de la liaison internet de secours.			
Acteurs impliqués: Francis Yelouassi, Gaël Daudin			
PROBLEMATIQUE SOULEVEES			
Basculement automatique vers la liaison de secours			
AXES DE PROGRES			
Amélioration de la résilience des moyens de transmissions.			
PLAN D'ACTION			
Action à entreprendre	Service en charge de l'action	Echéancier	Observations
Configuration de la liaison de secours en mode « load balancing »	Informatique	Septembre de 2013	RAS

## **4. Bilans et alternatives**

Nous présentons dans ce chapitre le bilan du projet ainsi que les alternatives puis un bilan personnel.

### **4.1. Bilan projet**

Dans le cadre de la mise en œuvre du plan de réduction des charges par Oryx Bénin SA, la solution précédemment étudiée par rapport à la réplication des données et qui impliquait une stratégie Falconstor a été jugée trop coûteuse. Il nous a donc été demandé de proposer une solution moins coûteuse. Ci-dessous présentée, l'étude réalisée à cet effet dans la rubrique alternative.

#### **4.1.1. Alternative**

Nous avons travaillé à réviser les objectifs de réplication afin de pouvoir réutiliser les anciens équipements du site secondaire. Nous envisageons d'installer une ligne internet ADSL sur le site secondaire avec des modules client légers Citrix.

##### **➤ Solution techniques DRP de Darest**

###### **Option n°1**

Cette solution Permet d'exploiter l'ensemble des éléments en place actuellement (serveurs ProLiant G7, Baie de stockage EMC VNX) pour équiper le site de replie. L'implémentation sur le site principal consiste en 2 serveurs ProLiant Gen8 et d'une baie de stockage Lefthand iSCSI Lefthand, cette solution permet d'allier la facilité de déploiement et la robustesse de la technologie iSCSI, à la performance et aux possibilités accrues des baies P4500 Lefthand.

Sur le site de secours, les équipements précédemment en production sont reconditionnés pour être intégrés dans un environnement « Lefthand » et permettre ainsi la mise en place d'une solution de continuité fiable. Chacun des serveurs G7, resteront équipés de serveurs VMware vSphere. Une machine virtuelle spéciale appelée Lefthand VSA (Virtual Software Appliance) sera installée localement sur les disques propres à chaque serveur vSphere et à ces VSA seront présentées des LUNs résidentes sur la baie EMC VNX (chaque VSA devant avoir ses propres LUNs dédiées). Les deux VSA seront alors paramétrées en un seul et même cluster Lefthand afin de permettre un

mirroring des données locales au site de replie. L'implémentation de la solution, pourra consister en la réplication synchrone ou asynchrone des données entre le cluster Lefthand du site principal et le cluster du site de replie. Cette réplication pourra être asservie par le temps et/ou construite sur la base de snapshot consistants des datastores VMware vSphere en fonction des possibilités de l'infrastructure de transmission entre les deux sites.

#### **Avantages de l'option n°1**

- Récupération des anciens équipements pour le DR
- Pilotage de la synchronisation des données entre les deux sites
- Facilité d'administration des baies Lefthand

#### **Inconvénients de l'option n°1**

- Pas de redondance sur le site principal. En cas de maintenance ou de problème sur la baie Lefthand physique, tout l'environnement doit être arrêté. Dans l'hypothèse où il ne serait pas possible de faire une réplication synchrone des données entre les deux sites, en cas de maintenance programmée, impossible de déclencher le DRP pour minimiser le trou de service vu les RTO/RPO applicables.
- Seulement deux connexions iSCSI de 1Gb seront disponibles sur le site principal.

#### **Option n°2**

Basée sur le même concept fonctionnel que la première option, la seconde solution proposée permet d'éliminer l'implémentation d'une appliance Lefthand physique sur le site principal. On conserve la possibilité de reconditionner les équipements précédemment utilisés en production sur le site de replie, l'implémentation propre à ce site reste identique à la version précédente. Sur le site principal, les deux nouveaux serveurs seront équipés en disques durs à hauteur de 7.2To de stockage bruts sur chaque machine. Ces deux machines se verront alors affectées une VSA Lefthand chacun, les deux VSA fonctionnant en cluster comme sur le site de replie. L'implémentation du DR reste la même que dans la solution 1.

### **Avantages de l'option n°2**

- Récupération des anciens équipements pour le DR
- Pilotage de la synchronisation des données entre les deux sites
- Facilité d'administration des baies Lefthand
- Réplication synchrone possible des données entre les deux VSA du site principal rendant possible une mise à jour des baies sans trous de service, ou une haute disponibilité de l'environnement.
- Fonctionnement des VSAs en mode Actif/Actif, chaque VSA participe à la performance du cluster
- Quatre (04) liens iSCSI de 1Gb disponibles sur le site principal

### **Inconvénient de l'option n°2:**

- Latence induite par l'utilisation des VSAs sur le site principal.

## **4.2. Bilan Personnel**

Le projet DRP OBSA a été pour moi l'occasion, d'approfondir ma connaissance, non seulement des aspects techniques du système d'information de l'entreprise, mais également d'affiner cette approche managériale qui permet de réellement mettre l'informatique au service des métiers. En effet, La phase d'étude d'impact sur l'activité a nécessité une forte interaction avec les différents responsables d'activité, qui ayant adhéré à l'idée de renforcer la résilience de l'entreprise, se sont pleinement investis à l'atteinte des objectifs.

La phase d'analyse de risque a été pour moi l'occasion d'évaluer réellement l'exposition du système d'information et d'exploiter la base de connaissance Méhari dont je découvrais toute la puissance.

La conception et la mise en œuvre de l'infrastructure optimisée, m'ont permis d'établir le lien entre l'analyse de risque et l'architecture du SI qui sont deux domaines apparemment transverses, mais en réalité complémentaires.

L'organisation du projet et les analyses techniques propres à la salle de repli ont été pleinement effectuées. La phase de rédaction des plans de continuité est en cours et une bonne partie des opérations sont en cours de réalisation.

Le comité de pilotage m'a permis d'apprendre à chaque étape de ce projet. En effet la longue expérience technique et managériale des membres de cette équipe m'a permis d'aller à l'essentiel, tout en tenant compte des détails et de mener à bien ce projet.

Par ailleurs, le projet DRP, constitue un vivier de ressources, pour le déploiement du plan de continuité d'activité à d'autres services d'OBSA; Je pense en priorité au service maintenance, pour la gestion des bras robots de chargement et le carrousel.

Enfin, rédiger mon mémoire d'ingénieur sur un sujet relatif à la continuité d'activité a été pour moi l'occasion d'acquérir des connaissances sur un sujet en vogue et qui n'a pas manqué de susciter en moi de la passion. Je pense que la continuité d'activité qui est une discipline relativement récente à de l'avenir.

## **Conclusion**

L'impulsion donnée par le top management au projet DRP, l'existence d'un cadre précisant les attentes d'un PCA et la disponibilité au sein du groupe des compétences nécessaires, ont favorisé, le bon déroulement du projet. Le retard accusé par le projet est imputable au projet OKAPI, initié dans le cadre du changement de statut juridique du groupe AOG.

Le projet DRP a donné lieu à la refonte du système informatique de la société, par la mise en place, d'un environnement virtualisé et la réorganisation complète du processus de sauvegarde des données. Cette refonte du système, a donné lieu à la stratégie de réplication des données entre les sites de la Direction et du dépôt qui constituent une formidable alternative à la continuité des activités.

L'analyse de risque et le bilan d'impact sur l'activité, tout en permettant de desceller les failles du système et l'impact d'éventuels sinistres, constituent des prémices, pour la mise en place d'un système de management de la sécurité du système d'information.

Enfin, en se dotant d'un DRP, OBSA s'inscrit dans la liste des entreprises, qui ont bien compris, je cite, que « Les crises de demain sont souvent le refus des questions d'aujourd'hui » (Patrick Lagadec).

## Références

### ▪ Bibliographie

- Emmanuel Besluau, 2011, Management de la continuité d'activité, édition Eyrolles
- Matthieu Bennasar, 2010, plan de continuité d'activité et SI, édition Dunod
- AFNOR, Plan de continuité d'activité, 2007
- Hervé Schauer Consultants ; Normes en sécurité, 2011
- CLUSIR, Plan de continuité d'activité, 2008
- AFNOR, Outil méthodologique
- CLUSIF, 2003, Plan de continuité d'activité, Stratégie et solution de secours du SI
- ENISA, 2008, Business and IT Continuity: Overview and Implementation Principles

### ▪ Webographie

<http://itil.fr/DRP/PCA/drppca-mettre-en-oeuvre-un-plan-de-continuite-dactivite.html>

<http://www.hsc.fr/presse/clubpca/LIVRE-BLANC-CCA.pdf>

<http://www.ssi-conseil.com/content/view/103/132/>

[http://www.ssi.gouv.fr/site\\_article45.html](http://www.ssi.gouv.fr/site_article45.html)

<http://www.clusif.asso.fr/fr/production/mehari/mehari.asp>

<http://www.altairconseil.fr/plan-de-continuite.html>

[http://www.duquesnegroup.com/PCA-Analyse-des-risques-et-Bilan-dImpact\\_a97.html](http://www.duquesnegroup.com/PCA-Analyse-des-risques-et-Bilan-dImpact_a97.html)

<http://www.techno-science.net/?onglet=glossaire&definition=704>

[http://www.accordance.fr/infoqualite/dossiers/dossiers.php?id\\_dossier=178](http://www.accordance.fr/infoqualite/dossiers/dossiers.php?id_dossier=178)

<http://www.solucom.fr/Publications>

<http://www.digital-network.net>

<http://www-igm.univ-mlv.fr/>

<http://www.bsigroup.fr/fr/Services-daudit-et-de-certification/>

<http://www.iso.org/iso/fr/home/>

<http://itil.fr/ITIL-V2/itil-v2-processus-de-gestion-de-la-continuite-de-service.html>

<http://www.solucominsight.fr/2012/07/>

## Index des figures

Figure n°1 : Présence géographique du Groupe OBSA.....	3
Figure n°2 : Vue partiel du terminal pétrolier d'OBSA .....	4
Figure n°3 : Vue partielle des produits et services d'OBSA .....	5
Figure n°4 : Extrait du PPM – Chapitre 3.....	6
Figure n°5 : Extrait du PPM – Chapitre 9.....	7
Figure n°6 : Concept du PCA .....	10
Figure n°7 : Schéma de crise .....	12
Figure n°8 : Volet du PCA.....	14
Figure n°9 : Etapes de mise en œuvre du PCA.....	28
Figure n°10 : Impact du facteur temps.....	21
Figure n°11 : Chronologie de crise .....	23
Figure n°12 : Matrice de risque .....	24
Figure n°13 : Démarche inductive.....	26
Figure n°14 : Démarche déductive .....	26
Figure n°15 : Cadre RMF .....	28
Figure n°16 : Alignement stratégique du PCA .....	30
Figure n°17 : Cluster de server .....	31
Figure n°18 : Avantages de la mise en cluster.....	32
Figure n°19 : Architecture du campus cluster .....	35
Figure n°20 : Architecture metropolitan cluster .....	35
Figure n°21 : Architecture du continental cluster.....	36
Figure n°22 : Extrait de référencement.....	42
Figure n°23 : Découpage du SI.....	48
Figure n°24 : Topologie réseau d'OBSA.....	51
Figure n°25 : Topologie – Forêt AOG.....	52
Figure n°26 : Extrait configuration Autocom .....	53
Figure n°27 : Grille d'évaluation de l'impact du risque risques.....	59
Figure n°28 : Grille d'évaluation de la sévérité du risque .....	60
Figure n°29 : Carte des zones sismiques .....	62
Figure n°30 : Aperçu Google Earth du terminal OBSA .....	63
Figure n°31 : Plan du réseau incendie d'OBSA .....	64
Figure n°32 : Extrait de rapport d'exercice incendie.....	64
Figure n°33 : Statut de potentialité .....	68
Figure n°34 : Statut de réduction du risque .....	72
Figure n°35 : Grille d'évaluation d'impact.....	73
Figure n°36 : Impact des menaces .....	74
Figure n°37 : Page d'accueil Méhari .....	89
Figure n°38 : Schéma de navigation – Méhari .....	89
Figure n°39 : Classification des services .....	90
Figure n°40 : Impact intrinsèque .....	91
Figure n°41 : Extrait du questionnaire d'audit.....	93
Figure n°42 : Extrait du panorama des gravités par scénario .....	93



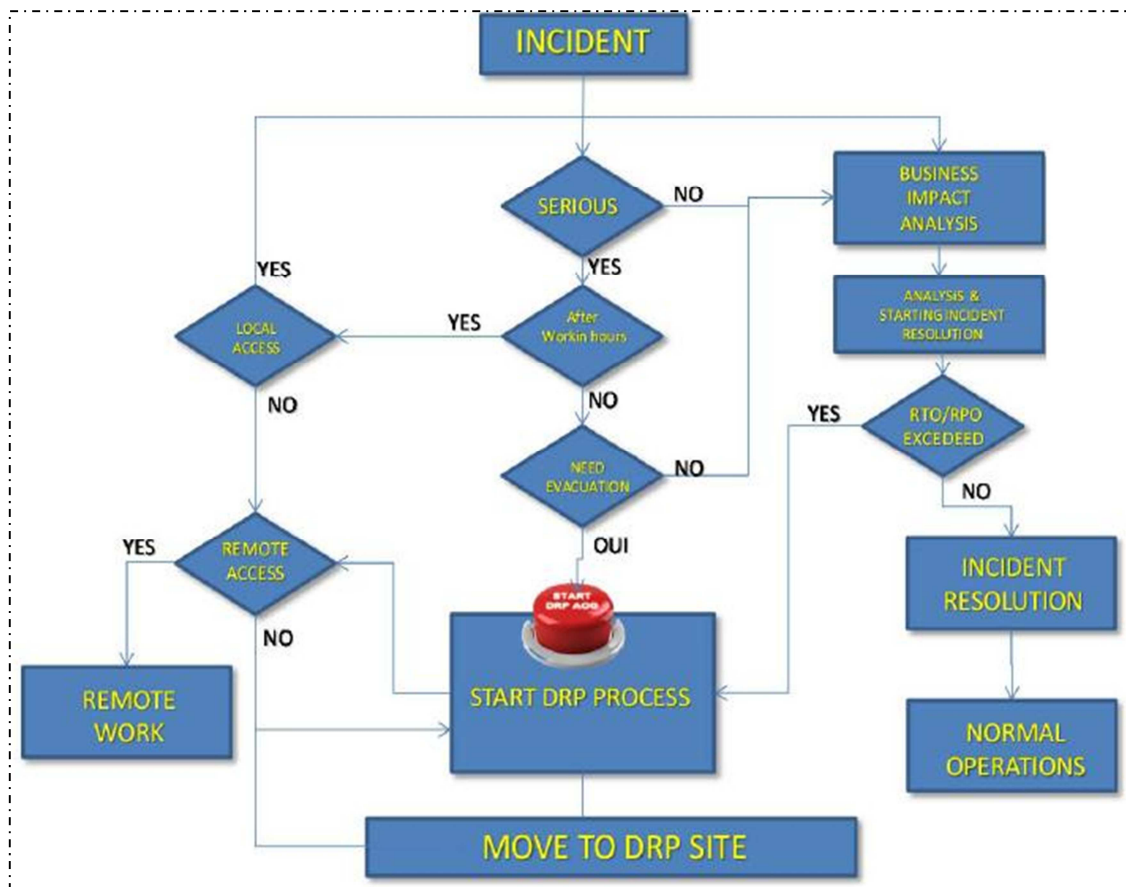
Figure n°43 : Extrait du tableau des évènements.....	94
Figure n°44 : Extrait des scénarios retenus.....	95
Figure n°45 : Ancienne configuration servers.....	99
Figure n°46 : Positionnement du Virtual center.....	102
Figure n°47 : Gestion ESX.....	103
Figure n°48 : Aperçu VM.....	104
Figure n°49 : Répartition des VM.....	105
Figure n°50 : LUN – SAN.....	106
Figure n°51 : LUN – Répartition.....	106
Figure n°52: Ecran Job setup.....	107
Figure n°53 : Règles de Template.....	108
Figure n°54 : Liste de sauvegarde.....	109
Figure n°55 : Extrait note de service.....	110
Figure n°56 : Algorithme de gestion du backup.....	110
Figure n°57 : Topologie OBSA après refonte.....	111
Figure n°58 : Infrastructure DRP.....	113
Figure n°59 : Login utilisateur.....	114
Figure n°60 : Stratégie Falconstor.....	114
Figure n°61: Etat de basculement.....	115
Figure n°62 : Retours à la normale.....	116

## Index des tableaux

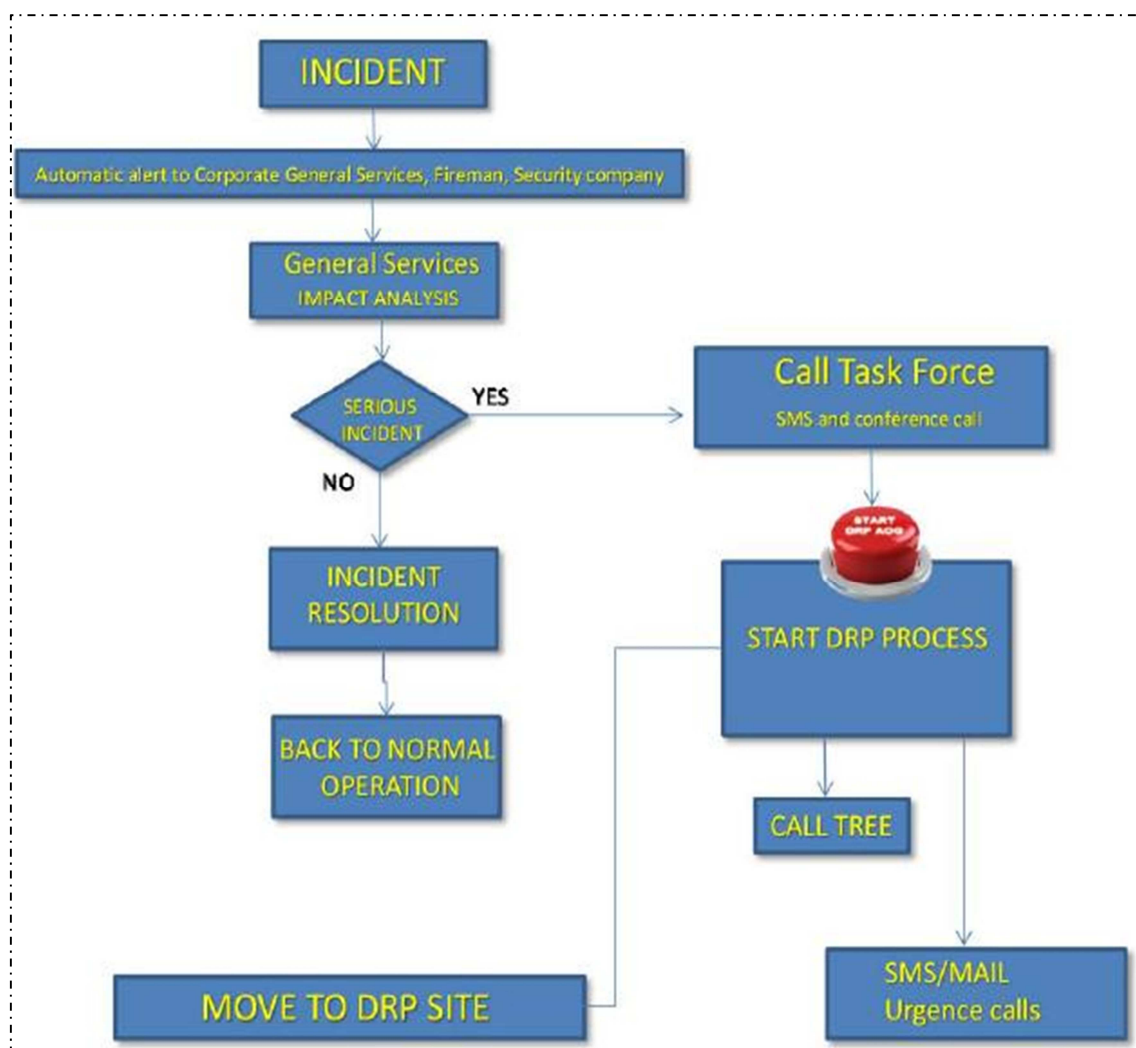
Tableau I: Fiche signalétique d'OBSA.....	5
Figure n II: Répartition du personnel d'OBSA au 31-12-12.....	6
Tableau III: Terminologie.....	12
Tableau IV : Phases du projet DRP.....	39
Tableau V: Livrables.....	42
Tableau VI: Extrait du planning du Projet DRP.....	45
Tableau VII: Extrait de l'inventaire Logiciel d'OBSA.....	54
Tableau VIII: Statut des mesures de protection.....	55
Tableau IV : Statut des mesures palliatives.....	56
Tableau X : Statut des mesures de récupération.....	56
Tableau XI : Statut des mesures de réduction du risque.....	57
Tableau XII : Statut d'exposition au risque.....	57
Tableau XIII statut des mesures dissuasives.....	58
Tableau XIV : Statut des mesures préventives.....	58
Tableau XV : Grille d'évaluation du statut de potentialité.....	59
Tableau XVI : Liste des menaces potentielles.....	61
Tableau XVII : Etat de réduction des impacts des sinistres.....	70
Tableau XVIII : Priorisation des scénarios de sinistre.....	71
Tableau XIX : Impact des menaces.....	72
Tableau XX : Sévérité u risque.....	74
Tableau XXI : Processus étudiés.....	77
Tableau XXII : Impacts financiers et opérationnels.....	85
Tableau XXIII : Processus critiques.....	86
Tableau XXIV : Configurations.....	86
Tableau XXV : RTO.....	87
Tableau XXVI : Détermination du RPO.....	87

## Annexe

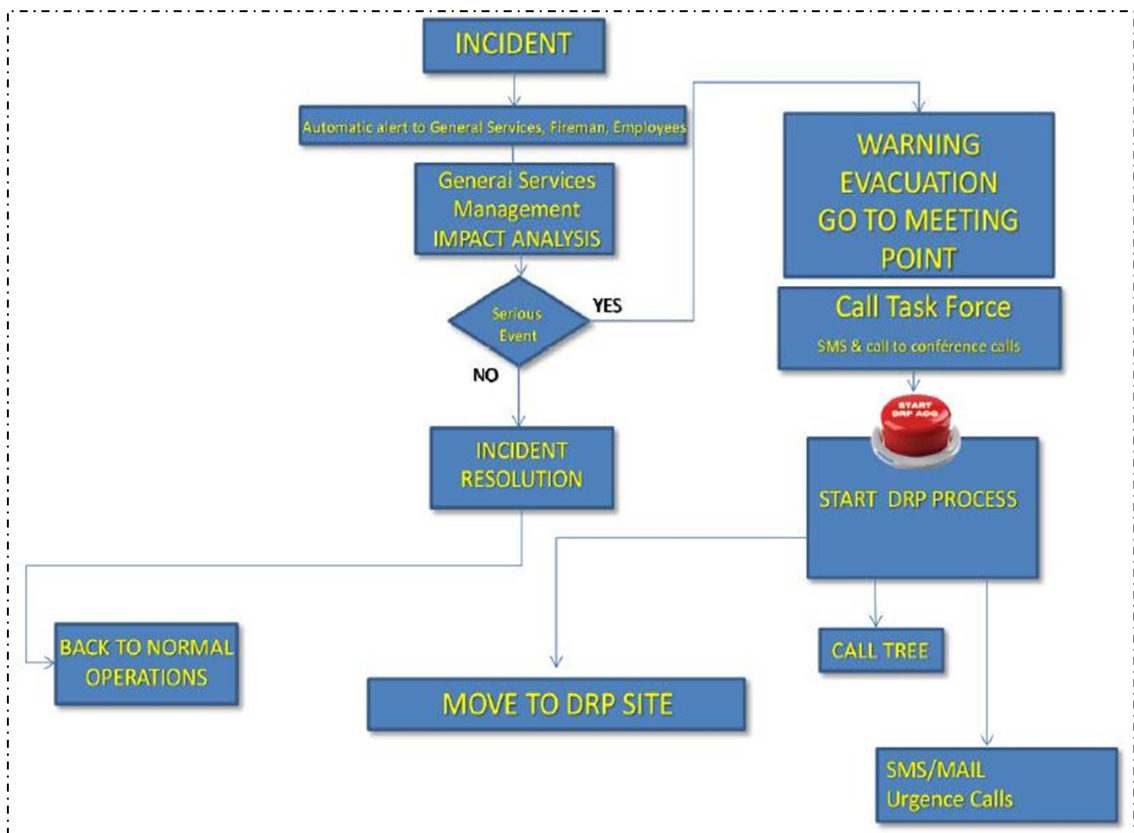
### ▪ Processus d'évaluation du Sinistre



- **Processus d'activation du DRP à une heure non ouvrée**



- **Processus d'activation du DRP à une heure ouvrée**



▪ **Tableaux de synthèses BIA**

→ **Tableau de classification des processus**

<b>Fonction</b>	<b>Processus métier</b>	<b>Priorité</b>
Opérateur	Confirmer chargement	CRITIQUE
	Libérer camion	CRITIQUE
Administration des ventes	Gérer commande client	CRITIQUE
	Gérer logistique	CRITIQUE
Comptabilité client	Gérer facturation client	CRITIQUE
	Mettre à jour fichier client	CRITIQUE
	Libérer commande	CRITIQUE
Comptabilité Fournisseur	Gérer facture fournisseur	CRITIQUE
Comptabilité Matière	Gérer stock	IMPORTANT
	Elaborer stock report	IMPORTANT
Comptabilité Générale	Paramétrer comptes	CRITIQUE
	Gérer fiscalité	CRITIQUE
GRH	Gérer Paie	IMPORTANT
Reporting et consolidation	Gérer consolidation	CRITIQUE
	Elaborer Reporting	CRITIQUE

→ **Tableau de synthèse des processus critiques**

<b>Fonction</b>	<b>Processus métier</b>	<b>Gravité</b>
Opérateur	Confirmer chargement	15
	Libérer camion	15
Administration des ventes	Gérer commande client	15
	Gérer logistique	10
Comptabilité client	Gérer facturation client	11
	Mettre à jour fichier client	12
	Libérer commande	11
Comptabilité Fournisseur	Gérer facture fournisseur	10
GRH	Gérer Paie	10
Reporting et consolidation	Gérer consolidation	10
	Elaborer Reporting	12

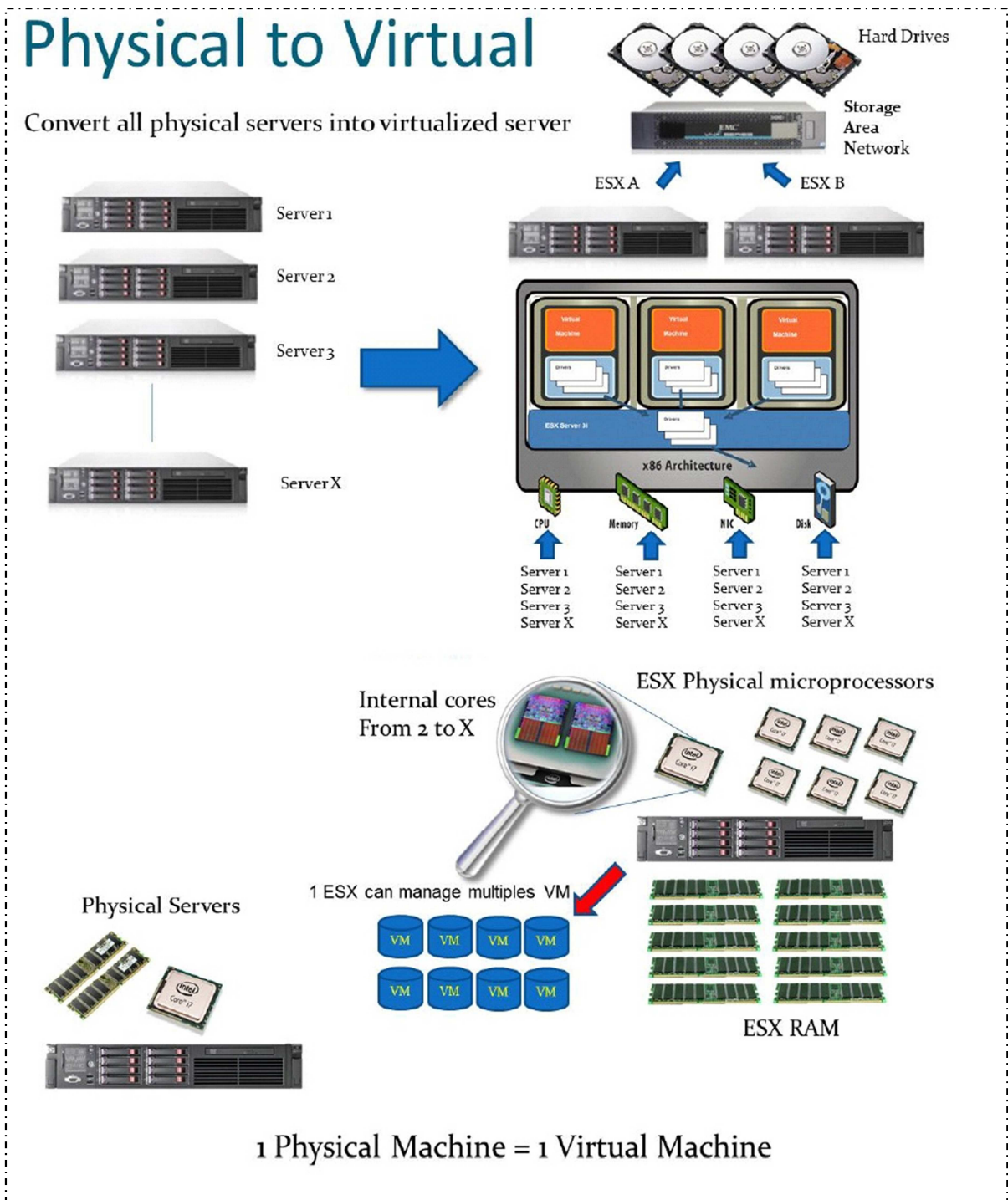
→ **Tableau de synthèse des applications et système critiques**

<b>Fonction</b>	<b>Processus métier</b>	<b>Application et systèmes critiques</b>
Opérateur	Confirmer chargement	- Téléphonie - ERP JDE sur le site de la Direction d'exploitation
	Libérer camion	- Système d'automatisation Alma sur site de la Direction d'exploitation - Messagerie Lotus Notes
Administration des ventes	Gérer commande client	- Téléphonie - ERP JDE sur le site de la Direction Générale
	Gérer logistique	- Messagerie Lotus Notes
Comptabilité client	Gérer facturation client	- Téléphonie - ERP JDE sur le site de la Direction Générale
	Mettre à jour fichier client	- Messagerie Lotus Notes
	Libérer commande	
Comptabilité Fournisseur	Gérer facture fournisseur	- Téléphonie - ERP JDE sur le site de la Direction Générale - Messagerie Lotus Notes
GRH	Gérer Paie	- Téléphonie - Logiciel Sage Saari - Messagerie Lotus Notes
Reporting et consolidation	Gérer consolidation	- Logiciel Vigilens - ERP JDE sur le site de la Direction Générale
	Elaborer Reporting	- Accès HFM - Messagerie Lotus Notes

→ **Tableau d'ajustement sur les MTD**

<b>Fonction</b>	<b>Processus métier</b>	<b>MTD</b>	<b>RTO</b>	<b>WRT</b>
Opérateur	Confirmer chargement	2,5	1,5	1
	Libérer camion	2	1,5	0,5
Administration des ventes	Gérer commande client	2,5	1,5	1
	Gérer logistique	2	1,5	0,5
Comptabilité client	Gérer facturation client	3	1,5	1,5
	Mettre à jour fichier client	2	1,5	0,5
	Libérer commande	2	1,5	0,5
Comptabilité Fournisseur	Gérer facture fournisseur	2,5	1,5	1
GRH	Gérer Paie	1,5	1	0,5
Reporting et consolidation	Gérer consolidation	4	3	1
	Elaborer reporting	2	1	1

- Principe technique de la virtualisation



▪ **Output de la base de connaissance MEHARI**

<b>MEHARI 2010</b>				
Version :	2.14			
Organisme :	Oryx Bénin SA			
Maîtrise d'ouvrage	DG OBSA			
Maîtrise d'oeuvre	Francis Yelouassi			
Responsable :	Daniel Nunez			
Rédacteur :	Francis Yelouassi			
Date début :				
Date fin :	08/03/2013			
Description du contexte :	Etude de risque dans le cadre du plan de continuité d'activité de la société OBSA.			

**Grilles d'élaboration des STATUS-I**

**1. Scénarios de type Disponibilité**

	II = 1	II = 2	II = 3	II = 4
C 4	1 1 1 1	C 4 2 2 1 1	C 4 2 2 1 1	C 4 2 2 2 1
O 3	1 1 1 1	O 3 2 2 1 1	O 3 3 2 2 1	O 3 3 3 2 1
N 2	1 1 1 1	N 2 2 2 2 1	N 2 3 3 2 1	N 2 4 3 2 1
F 1	1 1 1 1	F 1 2 2 2 1	F 1 3 3 2 1	F 1 4 3 2 1
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P A L L	P A L L	P A L L	P A L L

**2. Scénarios de type Intégrité**

	II = 1	II = 2	II = 3	II = 4
C 4	1 1 1 1	C 4 1 1 1 1	C 4 1 1 1 1	C 4 1 1 1 1
O 3	1 1 1 1	O 3 2 2 1 1	O 3 2 2 1 1	O 3 2 2 2 1
N 2	1 1 1 1	N 2 2 2 2 1	N 2 3 3 2 1	N 2 3 3 2 1
F 1	1 1 1 1	F 1 2 2 2 1	F 1 3 3 2 1	F 1 4 3 2 1
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
	P A L L	P A L L	P A L L	P A L L



Classification des données

Tableau T1		CLASSIFICATION DES DONNÉES																													
Processus métier, domaine applicatif ou domaine d'activité  Services communs à particulariser	FONCTION (descriptif)	Données applicatives (bases de données)			Données applicatives isolées, en transit Messages			Fichiers bureautiques partagés			Fichiers bureautiques personnels			Documents personnels		Listings ou états imprimés	Courrier électronique			Courrier postal Fax			Archives documentaires		Arhives informatiques			Données publiées (web ou interne)			Incl
		D	I	C	D	I	C	D	I	C	D	I	C	D	C	C	D	I	C	D	I	C	D	C	D	I	C	D	I	C	
Types d'actifs		D01	D01	D01	D06	D06	D06	D02	D02	D02	D03	D03	D03	D04	D04	D05	D07	D07	D07	D08	D08	D08	D09	D09	D10	D10	D10	D11	D11	D11	
<b>Processus métiers</b>																															
Domaine 1 : Confirmer Chargement	Opérateur	4	1	1	1	1	1	3	2	1	1	1	1	1	1	3	3	1	3	1	1	1	1	1	3	2	3	1	1	1	1
Domaine 2 : Libérer Camion	Opérateur	4	3	1	1	1	1	3	1	1	1	1	1	1	1	3	1	1	3	1	1	1	1	1	2	2	2				1
Domaine 3 : Gérer commande client	Administration des ventes	4	3	1	1	1	1	3	2	1	1	1	1	1	1	3	2	2	3	1	1	1	1	1	2	2	2				1
Domaine 4 : Gérer logistique	Administration des ventes	3	2	1	1	1	1	3	1	1	1	1	1	1	1	3	2	2	2	1	1	1	1	1	2	2	2				1
Domaine 5 : Gérer facturation client	Comptabilité Client	4	3	3	1	1	1	3	1	1	1	1	1	1	1	3	3	3	3	1	1	1	1	1	2	2	2				1
Domaine 6 : Mettre à jour fichier client	Comptabilité Client	4	3	1	1	1	1	2	3	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	2	2				1
Domaine 7 : Libérer commande	Comptabilité Client	4	1	2	1	1	1	1	1	1	1	1	1	1	1	2	3			1	1	1	1	1	2	2	2				1
Domaine 8 : Gérer facture fournisseur	Gérer facture Fournisseur	2	2	3	1	1	1	1	1	1	1	1	1	1	1	2	3	2	2	1	1	1	1	1	2	2	2				1
Domaine 9 : Gérer paie	GRH	3	3	4	1	1	1	3	3	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	2	2	2				1
Domaine 10 : Gérer Consolidation	Reporting et Consolidation	4	4	2	1	1	1	4	3	1	1	1	1	1	1	2	1	2	4	1	1	1	1	1	3	3	3				1
Domaine 11 : Elaborer reporting	Reporting et Consolidation	3	4	2	1	1	1	4	3	1	1	1	1	1	1	2	1	2	4	1	1	1	1	1	3	3	3				1
<b>Processus transverses</b>																															
Processus 1 :																															
Processus 2 :																															
Processus 3 :																															
Administration/ politique d'ensemble																															
Classification pour l'ensemble		4	4	4	1	1	1	4	3	1	1	1	1	1	1	3	3	3	4	1	1	1	1	1	3	3	3	1	1	1	
Classification pour le périmètre choisi		4	4	4	1	1	1	4	3	1	1	1	1	1	1	3	3	3	4	1	1	1	1	1	3	3	3	1	1	1	
<p>La synthèse des classifications (maximum) par colonne est effectuée automatiquement : pour ajouter ou supprimer des domaines utiliser les fonctions " insérer " une ligne ou "supprimer " une ligne.</p> <p>La classification (maximum de chaque colonne) est reportée dans le tableau d'impact intrinsèque, pour chaque type de données dans la colonne correspondant au critère de classification (D, I ou C)</p>																															

Classification des services

Tableau T2		CLASSIFICATION DES SERVICES																	
Processus métier, application ou domaine applicatif Services communs	FONCTION (descriptif)	Services du réseau étendu		Services du réseau local		Services applicatifs			Services bureautiques communs		Equipe-ments mis à la disposition des utilisateurs	Services systèmes Communs (Systèmes, périfs, etc.)		Services de publication sur site web		Services généraux environnement de travail	Services télécom		
		D	I	D	I	D	I	C	D	I	D	D	I	D	I	D	D	I	
		R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S04	S04	S05	S05	G01	G02	G02	
Nom de colonne pour formules Classif		R01	R01	R02	R02	S01	S01	S01	S02	S02	S03	S04	S04	S05	S05	G01	G02	G02	
<b>Processus métiers</b>																			
Domaine 1 : Confirmer Chargement	Opérateur	2	1	4	3	4	4	2	3	1	4	4	1	1	1	2	3	1	
Domaine 2 : Libérer Camion	Opérateur	2	1	4	3	4	4	2	2	1	4	3	1	1	1	2	3	1	
Domaine 3 : Gérer commande client	Administration des ventes	2	1	4	3	4	4	2	2	2	4	1	1	1	1	2	3	3	
Domaine 4 : Gérer logistique	Administration des ventes	2	1	4	3	2	4	2	4	3	4	1	1	1	1	2	3	2	
Domaine 5 : Gérer facturation client	Comptabilité Client	3	1	4	3	4	4	2	3	3	4	4	1	1	1	2	3	2	
Domaine 6 : Mettre à jour fichier client	Comptabilité Client	2	1	4	3	4	4	2	1	1	4	1	1	1	1	2	3	1	
Domaine 7 : Libérer commande	Comptabilité Client	2	1	4	3	4	4	2	1	1	4	1	1	1	1	2	3	2	
Domaine 8 : Gérer facture fournisseur	Gérer facture Fournisseur	3	1	3	2	4	4	2	3	4	4	3	1	1	1	2	3	2	
Domaine 9 : Gérer paie	GRH	1	1	2	2	4	4	4	3		4	3	1	1	1	2	3	1	
Domaine 10 : Gérer Consolidation	Reporting et Consolidation	4	3	3	4	4	4	4	4	3	4	2	1	1	1	2	4	3	
Domaine 11 : Elaborer reporting	Reporting et Consolidation	4	3	3	4	3	4	4	4	3	4	3	1	1	1	2	4	3	
<b>Processus transverses</b>																			
Processus 1 :																			
Processus 2 :																			
Processus 3 :																			
Administration/ politique d'ensemble																			
<b>Classification pour l'ensemble</b>		4	3	4	4	4	4	4	4	4	4	4	1	1	1	2	4	3	
<b>Classification pour le périmètre</b>		4	3	4	4	4	4	4	4	4	4	4	1	1	1	2	4	3	
<b>LES CRITERES DE CLASSIFICATION SONT :</b>																			
D : Disponibilité																			
I : Intégrité																			
C : Confidentialité																			
La synthèse des classifications (maximum) par colonne est effectuée automatiquement : pour ajouter ou supprimer des domaines utiliser les fonctions " insérer " une ligne ou "supprimer " une ligne.																			
La classification (maximum de chaque colonne) est reportée dans le tableau d'impact intrinsèque, pour chaque type de service dans la colonne correspondant au critère de classification (D, I ou C)																			

▪ Classification des processus de management

Tableau T3		CLASSIFICATION DES PROCESSUS DE MANAGEMENT					
Processus métier, application ou domaine applicatif Services communs	FONCTION (descriptif)	Protection des renseignements personnels	Communication financière	Vérification de la comptabilité informatisée	Protection de la propriété intellectuelle	Protection des systèmes informatisés	Sécurité des personnes et protection de l'environnement
		E	E	E	E	E	E
Nom de colonne pour formules Classif		C01	C02	C03	C04	C05	C06
<b>Processus métiers</b>							
Domaine 1 : Confirmer Chargement	Opérateur	1	1	1	1	3	2
Domaine 2 : Libérer Camion	Opérateur	1	1	1	1	3	2
Domaine 3 : Gérer commande client	Administration des ventes	1	1	1	1	3	2
Domaine 4 : Gérer logistique	Administration des ventes	1	1	1	1	2	2
Domaine 5 : Gérer facturation client	Comptabilité Client	1	4	4	1	3	2
Domaine 6 : Mettre à jour fichier client	Comptabilité Client	1	1	1	1	3	2
Domaine 7 : Libérer commande	Comptabilité Client	1	1	1	1	3	2
Domaine 8 : Gérer facture fournisseur	Gérer facture Fournisseur	1	4	4	1	3	2
Domaine 9 : Gérer paie	GRH	1	1	1	1	3	2
Domaine 10 : Gérer Consolidation	Reporting et Consolidation	1	4	4	1	3	2
Domaine 11 : Elaborer reporting	Reporting et Consolidation	1	4	4	1	3	2
<b>Processus transverses</b>							
Processus 1 :							
Processus 2 :							
Processus 3 :							
Administration/ politique d'ensemble							
<b>Classification pour l'ensemble</b>		1	4	4	1	3	2
<b>Classification pour le périmètre</b>		1	4	4	1	3	2
<p><b>LE SEUL CRITERE DE CLASSIFICATION EST :</b>  <b>E : Efficience (des processus de management pour être conforme aux exigences légales, réglementaires ou contractuelles, dans le domaine considéré)</b></p> <p><b>La synthèse des classifications (maximum) par colonne est effectuée automatiquement : pour ajouter ou supprimer des domaines utiliser les fonctions " insérer " une ligne ou "supprimer " une ligne.</b>  <b>La classification (maximum de chaque colonne) est reportée dans le tableau d'impact intrinsèque, pour chaque type de processus de management dans la colonne correspondant au critère de classification (E)</b></p>							

- Thèmes de sécurité

Thèmes de sécurité			Cotatio n actuell	Cotatio n finale
N° Libellé	Services appelés			
A1	Rôles et structures	01A, 01D	1,0	1,0
A2	Sensibilisation et formation à la sécurité, Gestion des ressources humaines	01B, 01C, 12D02	1,0	1,2
B1	Contrôles d'accès physiques (sites, bâtiments et locaux)	02A, 02C, 03B	1,0	1,0
B2	Risques divers	02B, 03A, 03C, 03D	1,2	2,9
C1	Architecture réseaux et systèmes	04A01, 05A01, 05A02, 07D, 09E01	1,0	2,0
C2	Contrôles des échanges	04C, 05C, 12D03	1,0	1,0
D1	Contrôle d'accès logique	04B, 05B, 06C01, 06C02, 07A, 07B, 08F01, 08F02, 09A, 11E01, 11E02, 12E01, 12E02	1,0	1,0
D2	Sécurité des données	08A05, 08D07, 09B, 09C, 09D, 09F, 09H, 11B, 11C, 11D06	1,0	1,1
E1	Procédures d'exploitation	04A02, 04A03, 05A03, 05A04, 06A, 06B, 06C04, 08A01 à 08A04, 08A06, 08A08, 08A09, 08B, 08D03, 08D10, 11A, 12A, 12B, 12D01	0,9	1,3
E2	Gestion des supports	08C, 08H	1,0	1,8
E3	Protection des documents et des informations écrites	02D, 08A07	1,0	1,0
F1	Plan de secours	01E, 04A05, 05A06, 08D06, 09E02, 11D07, 12C04	0,3	2,6
F2	Sauvegarde	04A04, 05A05, 08D04, 08D05, 08D09, 11D03, 11D04, 11D05, 12C03	0,6	2,6
F3	Maintenance	04A02, 04A06, 05A03, 05A07, 08D01, 08D02, 08D08, 09E03, 11D01, 11D02, 12C01, 12C02, 12C05	0,8	2,5
G1	Projets et développements	10A, 10B	1,0	1,2
H1	Détection et gestion des incidents	04D, 05D, 06C03, 07C, 08E, 08F03, 09G, 11E03, 12E03	0,8	1,6
I1	Gestion des audits	06D, 08G	1,0	1,0
J1	Gestion de la conformité	13	1,0	1,0
K1	Système de management de la sécurité de l'information	14	1,0	1,0

■ Panorama des gravités

Panorama des gravités de scénarios					Disponibilité				Intégrité				Confidentialité						
Actifs de type Données et informations					Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4	Gr. 1	Gr. 2	Gr. 3	Gr. 4			
<b>Données et informations</b>																			
D01	Fichiers de données ou bases de données applicatives				5	7	0	0	>	0	0	0	0	>	0	0	0	0	>
D02	Fichiers bureautiques partagés				3	3	0	0	>	0	0	0	0	>	0	0	0	0	>
D03	Fichiers bureautiques personnels (gérés dans environnement personnel)				0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D04	Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles				0	0	0	0	>					>	0	0	0	0	>
D05	Listings ou états imprimés des applications informatiques								>					>	0	0	0	0	>
D06	Données échangées, écrans applicatifs, données individuellement sensibles				0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D07	Courrier électronique				0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D08	Courrier postal et télécopies				0	0	0	0	>	0	0	0	0	>	0	0	0	0	>
D09	Archives patrimoniales ou documentaires				0	0	0	0	>					>	0	0	0	0	>
D10	Archives informatiques				0	4	0	0	>	0	0	0	0	>	0	0	0	0	>
D11	Données et informations publiées sur des sites publics ou internes				0	0	0	0	>	0	0	0	0	>					>
<b>Actifs de type Services</b>																			
<b>Services généraux communs</b>																			
G01	Environnement de travail des utilisateurs				0	0	0	0	>					>					>
G02	Services de télécommunication (voix, télécopies, visioconférence, etc.)				4	5	0	0	>	0	0	0	0	>					>
<b>Services informatiques et télécom</b>																			
R01	Service du réseau étendu				4	5	0	0	>	0	0	0	0	>					>
R02	Service du réseau local				4	5	0	0	>	0	0	0	0	>					>
S01	Services applicatifs				7	14	0	0	>	0	0	0	0	>	0	0	0	0	>
S02	Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)				7	14	0	0	>	0	0	0	0	>					>
S03	Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)				0	0	0	0	>					>					>
S04	Services systèmes communs : messagerie, archivage, impression, édition, etc.				0	0	0	0	>	0	0	0	0	>					>
S05	Services de publication d'informations sur un site web interne ou public				0	0	0	0	>	0	0	0	0	>					>
<b>Actifs de type Processus de management</b>																			
<b>Non conformité à la loi ou à la réglementation</b>																			
C01	Conformité à la loi ou aux réglementations relatives à la protection des renseignements				0	0	0	0	>					>					>
C02	Conformité à la loi ou aux réglementations relatives à la communication financière				0	0	0	0	>					>					>
C03	Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée				0	0	0	0	>					>					>
C04	Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle				0	0	0	0	>					>					>
C05	Conformité à la loi relative à la protection des systèmes informatisés				0	0	0	0	>					>					>
C06	Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement				0	0	0	0	>					>					>
<b>Nombre de scénarios:</b>					34	57	0	0		0	0	0	0		0	0	0	0	

▪ **Vulnérabilité par type d'actif**

Type d'actif secondaire	Type de dommage subi	Type de vulnérabilité	Critère DICE	Code	Sélection
<b>Catégorie : Service</b>					
Configuration logicielle	Altération	Possibilité d'altération des configurations logicielles (logiciels et paramètres)	D et I	Cfl.alt	0
	Non fonctionnement	Possibilité de non fonctionnement intrinsèque d'un logiciel (bug)	D	Cfl.bug	0
	Divulgateion de logiciel	Possibilité de diffusion de fichier de logiciel	C	Cfl.dif	0
	Effacement	Possibilité d'effacement de configurations logicielles	D	Cfl.eff	1
	Défaut d'autorisation	Possibilité de blocage par défaut d'autorisation (défaut de licence)	I	Cfl.lic	0
	Pollution	Possibilité de pollution des configurations logicielles	I	Cfl.pol	0
Compte ou moyen d'accès au service	Blocage	Possibilité de blocage des comptes utilisateurs	D	Cpt.blo	0
	Disparition	Possibilité de perte des moyens nécessaires à la connexion au service	D	Cpt.dis	1
Equipement matériel	Destruction	Possibilité de destruction d'un équipement	D	Eq.des	1
	Non fonctionnement	Possibilité de non fonctionnement d'un équipement	D	Eq.hs	1
	Non maintien en opération	Possibilité de non maintien en opération d'un équipement	D	Eq.mo	0
Locaux	Indisponibilité	Possibilité d'inaccessibilité des locaux	D	Loc.ina	1
Media support de logiciel	Destruction	Possibilité de destruction de media support de logiciel	D	Med.des	1
	Disparition	Possibilité de disparition de media support de logiciel	D	Med.dis	1
	Echange	Possibilité de disparition de media support de logiciel	I	Med.ech	1
	Inexploitabilité	Possible inexploitabilité de media support de logiciel	D	Med.ine	1
Moyens de servitude	Indisponibilité	Possibilité d'indisponibilité de moyens de servitude nécessaires	I	Ser.hs	0
<b>Catégorie : données</b>					
Moyen d'accès aux données	Disparition	Possibilité de disparition d'un moyen nécessaire pour l'accès aux données (clés logiques ou physiques)	D	Cle.dis	0
Données en transit, messages, écrans	Altération	Possibilité d'altération de données en transit ou messages	I	Dtr.alt	0
	Divulgateion	Possibilité de duplication (et divulgation) de données en transit, messages, écrans	C	Dtr.div	1
	Perte	Possibilité de perte de données en transit ou messages	D et C	Dtr.per	1
Fichier support de données	Altération	Possibilité d'altération du fichier support de données	I	Fic.alt	1
	Divulgateion	Possibilité de duplication ou diffusion (et divulgation) de fichier support de données	C	Fic.dif	0
	Effacement	Possibilité d'effacement du fichier support de données	D	Fic.eff	1
	Pollution	Possibilité de pollution (lente) des données du fichier	D	Fic.pol	0
Media support de données	Destruction	Possibilité de destruction de media support de données	D	Med.des	1
	Disparition	Possibilité de disparition de media support de données	D et C	Med.dis	1
	Duplication	Possibilité de duplication (et divulgation) de media support de données	D et C	Med.dup	0
	Echange	Possibilité d'échange de media support de données	D et C	Med.ech	0
	Inexploitabilité	Possible inexploitabilité de media support de données	D	Med.ine	1
<b>Catégorie : processus de management</b>					
Procédures et directives	Inefficience	Possibilité que les procédures appliquées soient inefficaces (vis-à-vis des obligations légales, réglementaires ou contractuelles)	E	Pro.inf	0

▪ Analyse détaillé serveurs

Nom du serveur	Adresse IP	Rôles	Type de serveur	Taille de RAM (Go)	Taille de disques durs (Go)	Partition (Go)	Taille restante (Go)	Machine virtualisée	Commentaire	Date d'Acquisition
DWBJCOO1-400	172.18.26.21	* Serveur lotus notes * Serveur VM ware * Serveur de fichiers	HP Proliant DL385 (Quad 2,4 GHZ AMD)	3,83	Disk 0: 9,76	C: 9,76	1,08	Non		2006
						D: 17,58	10,51			
					Disk 1: 25,38	E: 7,81	3,82			
					Disk 2: 32,67	Y: 32,67	7,3			
					Disk 3: 78,12	F: 78,12	3,39			
						G: 25,39	5,09			
	I: 32,14	10,71								
		H: 137,79	82,88							
DWBJCOO1-201	172.18.26.25	* Serveur d'impression * Serveur de Fichier		1,01	Disk 0: 7,99	C: 7,99	2,69	Oui	Sur la partition Y du DWBJCOO1-400	
DWBJCOO1-001	172.18.26.20	AD - Serveur de domaine	Accès limité au downstream administrator					Oui	Sur la partition Y du DWBJCOO1-400	
DWBJCOO1-600	172.18.26.22	* Serveur Vmware * Serveur de Sauvegarde	HP Proliant DL385 (Quad 2,4 GHZ AMD)	5,83	Disk 0: 9,75	C: 9,75	3,03	Non		2006
					Disk 1: 1,53	F: 19,53	19,21			
					Disk 2: 29,29	D: 29,29	17,87			
					Disk 3: 77,08	Y: 77,08	7,01			
					Disk 4: 33,91	W: 33,91	20,83			
DWBJCOO1-401	172.18.26.23	Serveur de déploiement JDE		2	Disk 0: 7,99	C: 7,99	2,13	Oui	Sur la partition Y du DWBJCOO1-600	
					Disk 1: 60	F: 60	8,03			
DWBJCOO1-403	172.18.26.27	Terminal Serveur Web JDE		1	Disk 0: 7,99	C: 7,99	1,54	Oui	Sur la partition Y du DWBJCOO1-600	
					Disk1: 4	D: 4	1,87			
DWBJCOO2-402	172.18.16.24	JDE * Serveur de base de données	HP Proliant DL385 (Quad 2,4 GHZ AMD)	7,83	Disk 0: 9,75	C: 9,75	1,76	Non		2006
					Disk 1: 39,06	D: 39,06	25,04			
					Disk 2: 19	E: 19	17,21			
					Disk 3: 67,83	F: 67,83	1,09			
DWBJCOO2-404	172.18.28.28	* Serveur Vmware * Serveur de fichiers	Compaq proliant ML370 (Intel Pentium III)	1,25	Disk 0: 33,91	C: 33,91	23,01	Non		
					Disk 1: 39,06	Y: 39,06	28,31			
						D: 19,53	19,47			
					Disk 2: 62,68	E: 43,15	31,22			
DWBJCOO2-004	172.18.28.11	AD - Serveur de domaine	Accès limité au downstream administrator					Oui	Sur la partition Y du DWBJCOO2-404	2002

▪ **Tableau des évènements**

<b>Tableau des évènements</b>			<b>Nombre de scénarios par niveau de gravité</b>				
<b>Type</b>	<b>Code type</b>	<b>Évènement</b>	<b>Code</b>	<b>Gr 1</b>	<b>Gr 2</b>	<b>Gr 3</b>	<b>Gr 4</b>
Absence accidentelle de personnel	AB.P	Absence de personnel de partenaire	AB.P.Pep	0	0	0	0
		Absence de personnel interne	AB.P.Per	0	0	0	0
Absence ou indisponibilité accidentelle de service	AB.S	Absence de service : Énergie	AB.S.Ene	0	0	0	0
		Absence de service : Climatisation	AB.S.Cli	0	0	0	0
		Absence de service : locaux	AB.S.Loc	0	0	0	0
		Absence de maintenance applicative ou maintenance app. impossible	AB.S.Maa	0	0	0	0
		Absence de maintenance système ou maintenance système impossible	AB.S.Mas	0	0	0	0
Accident grave d'environnement	AC.E	Foudroiement	AC.E.Fou	5	0	0	0
		Incendie	AC.E.Inc	12	0	0	0
		Inondation	AC.E.Ino	8	4	0	0
Accident matériel	AC.M	Panne d'équipement informatique ou télécom	AC.M.Equ	0	0	0	0
		Panne d'équipement de servitude	AC.M.Ser	0	0	0	0
Absence volontaire de personnel	AV.P	Conflit social avec grève	AV.P.Gre	0	0	0	0
Erreur de conception	ER.L	Bug bloquant dû à une erreur de conception ou d'écriture de programme (interne)	ER.L.Lin	0	0	0	0
Erreur matérielle ou de comportement du personnel	ER.P	Perte ou oubli de document ou de media	ER.P.Peo	0	0	0	0
		Erreur de manipulation ou dans le suivi d'une procédure	ER.P.Pro	0	0	0	0
		Erreur de saisie ou de frappe	ER.P.Prs	0	0	0	0
Incident dû à l'environnement	IC.E	Dégât dû au vieillissement	IC.E.Age	0	0	0	0
		Dégât des eaux	IC.E.De	9	4	0	0
		Surcharge électrique	IC.E.Pol	0	0	0	0
		Dégât dû à la pollution	IC.E.Se	0	0	0	0
Incident logique ou fonctionnel	IF.L	Incident d'exploitation	IF.L.Exp	0	0	0	0
		Bug bloquant dans un logiciel système ou un progiciel	IF.L.Lsp	0	0	0	0
		Saturation bloquante pour cause externe (ver)	IF.L.Ver	0	0	0	0
		Virus	IF.L.Vir	0	0	0	0
Malveillance menée par voie logique ou fonctionnelle	MAL	Attaque en blocage de compte	MAL.Blo	0	0	0	0
		Effacement volontaire ou pollution massive de configurations systèmes	MAL.Cfg	0	0	0	0
		Effacement volontaire direct de supports logiques ou physiques	MAL.Del	0	0	0	0
		Captation électromagnétique	MAL.Ele	0	0	0	0
		Falsification logique (données ou fonctions)	MAL.Fal	0	0	0	0
		Création de faux (messages ou données)	MAL.Fau	0	0	0	0
		Rejeu de transaction	MAL.Rej	0	0	0	0
		Saturation malveillante d'équipements informatiques ou réseaux	MAL.Sam	0	0	0	0
		Destruction logique totale (fichiers et leurs sauvegardes)	MAL.Tot	0	0	0	0
		Détournement logique de fichiers ou données (téléchargement ou copie)	MAL.Vol	0	0	0	0
Malveillance menée par voie physique	MAP	Manipulation ou falsification matérielle d'équipement	MAP.Fal	0	0	0	0
		Terrorisme	MAP.Ter	0	5	0	0
		Vandalisme	MAP.Van	0	20	0	0
		Vol physique	MAP.Vol	0	24	0	0
Procédures non conformes	PR.N	Procédures inadéquates	PR.N.Api	0	0	0	0
		Procédures inappliquées par manque de moyens	PR.N.Naa	0	0	0	0
		Procédures inappliquées par méconnaissance	PR.N.Nam	0	0	0	0
		Procédures inappliquées volontairement	PR.N.Nav	0	0	0	0



▪ Impact intrinsèque

Tableau d'Impact Intrinsèque				Sélection d'actifs
Actifs de type Données et informations	D	I	C	
<i>Données et informations</i>				
D01 Fichiers de données ou bases de données applicatives	4	4	4	1
D02 Fichiers bureautiques partagés	4	3	1	1
D03 Fichiers bureautiques personnels (gérés dans environnement personnel)	1	1	1	0
D04 Informations écrites ou imprimées détenues par les utilisateurs, archives	1		1	0
D05 Listings ou états imprimés des applications informatiques			3	0
D06 Données échangées, écrans applicatifs, données individuellement sensibles	1	1	1	0
D07 Courrier électronique	3	3	4	1
D08 Courrier postal et télécopies	1	1	1	0
D09 Archives patrimoniales ou documentaires	1		1	0
D10 Archives informatiques	3	3	3	1
D11 Données et informations publiées sur des sites publics ou internes	1	1	1	0
Actifs de type Services	D	I	C	
<i>Services généraux communs</i>				
G01 Environnement de travail des utilisateurs	2			0
G02 Services de télécommunication (voix, télécopies, visioconférence, etc.)	4	3		1
<i>Services informatiques et réseaux</i>				
R01 Service du réseau étendu	4	3		1
R02 Service du réseau local	4	4		1
S01 Services applicatifs	4	4	4	1
S02 Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)	4	4		1
S03 Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	4			0
<b>Nota : Considérer ici la perte massive de ces services et non celle d'un seul utilisateur</b>				
S04 Services systèmes communs : messagerie, archivage, impression, édition, etc.	4	1		0
S05 Services de publication d'informations sur un site web interne ou public	1	1		0
Actifs de type Processus de gestion	E			
<i>Processus de gestion de la conformité à la loi ou à la réglementation</i>				
C01 Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels	1			0
C02 Conformité à la loi ou aux réglementations relatives à la communication financière	4			0
C03 Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée	4			0
C04 Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle	1			0
C05 Conformité à la loi relative à la protection des systèmes informatisés	3			0
C06 Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement	2			0
Nota : Les cases grisées correspondent à des cas dans lesquels il n'y a généralement pas de classification à effectuer et pour lesquels il n'y a pas de scénario de risque dans la base Méhari.				
<b>Il faut mettre 0 dans la colonne F (sélection d'actifs) pour dé-sélectionner l'actif correspondant.</b>				
Légende :				
D	Disponibilité			
I	Intégrité			
C	Confidentialité			
E	Efficience (des processus de gestion, vis-à-vis de la conformité aux législations ou aux règlements). Pour ce critère, la grille de décision "Scénarios de type Limitable" pour l'impact sera utilisée.			

<b>Introduction</b> .....	1
1. Contexte.....	2
1.1. Présentation de l'entreprise.....	2
1.1.1. Profile du Groupe AOG .....	2
1.1.2. Présence géographique.....	2
1.1.3. Oryx Bénin SA .....	3
1.1.3.1. Le terminal pétrolier .....	4
1.1.3.2. L'activité GPL .....	4
1.1.3.3. L'activité Lubrifiant .....	5
1.1.3.4. Les stations-services.....	5
1.1.4. Organisation de la DSI.....	5
1.1.4.1. Objectif.....	5
1.1.4.2. Décentralisation .....	5
1.1.4.3. Plans transversaux .....	6
1.1.4.4. Reporting.....	6
1.2. Contexte de plan de continuité.....	6
1.2.1. L'existant .....	6
1.2.2. Synthèse .....	7
<b>2. Etat de l'art de la continuité d'activité</b> .....	9
2.1. Définition .....	9
2.2. Terminologie.....	10
2.3. Principes.....	10
2.4. Piliers du PCA .....	11
2.4.1. L'organisation de gestion de crise.....	11
2.4.2. Le système documentaire .....	13
2.4.3. Stratégie de prévention et de préparation.....	13
2.4.4. La solution Technique de continuité .....	13
2.5. Volets du PCA .....	14
2.6. Normes et standards.....	15
2.7. Démarche PCA .....	20
2.7.1. Analyse d'impact sur l'activité .....	20
2.7.1.1. Définition.....	20
2.7.1.2. Etapes de l'analyse d'impact .....	21
2.7.2. Analyse de risque .....	23
2.7.2.1. Définition.....	23
2.7.2.2. Mesure du risque .....	24
2.7.2.3. Etapes de l'analyse de risque.....	24
2.7.2.4. Méthode d'analyse de risques .....	25
2.7.2.4.1. Démarche d'investigation.....	26
2.7.2.4.2. Outils méthodologiques.....	26
2.7.3. Stratégie de continuité.....	29
2.7.4. Procédures de continuité .....	30
2.7.5. Tests .....	30
2.8. Infrastructures techniques .....	31

2.8.1. Les techniques .....	31
2.8.1.1.La mise en cluster.....	31
2.8.1.2.La réplication.....	32
2.8.1.3.La sauvegarde distante .....	33
2.8.1.4.La journalisation distante .....	33
2.8.1.5.La virtualisation.....	33
2.8.2. Typologie .....	33
2.8.3. Topologies.....	34
<b>3. Réalisation pratique .....</b>	<b>37</b>
3.1.Cadrage du projet DRP .....	37
3.1.1. Rappel du contexte .....	37
3.1.2. Enjeux et objectif .....	37
3.1.3. Périmètre du projet .....	38
3.1.4. Démarche .....	38
3.1.5. Organisation du projet.....	39
3.1.5.1.Comité de pilotage.....	39
3.1.5.2.Comité opérationnel .....	39
3.1.5.3.Equipe projet .....	39
3.1.6. Les livrables .....	40
3.1.7. Gestion de la documentation .....	42
3.1.7.1.Référencement .....	42
3.1.7.2.Stockage des documents.....	43
3.1.7.3.Circuit des documents .....	43
3.1.8. Planning prévisionnel .....	43
3.2.Cartographie du SI .....	45
3.2.1. Découpage du SI .....	45
3.2.1.1.Le SI opérationnel .....	45
3.2.1.2.Le SI d'aide à la décision .....	46
3.2.1.3.Le SI de communication.....	46
3.2.2. Architecture réseau.....	49
3.2.2.1.L'accès à internet.....	53
3.2.2.2.Les autocommutateurs.....	53
3.2.2.3.Les Logiciels .....	53
3.3.Cartographie des sinistres .....	55
3.3.1. Grille d'évaluation.....	55
3.3.1.1.Métriques des mesures de protection .....	55
3.3.1.2.Métrique des mesures palliatives .....	56
3.3.1.3.Métriques des mesures de récupération.....	56
3.3.1.4.Métrique des mesures de réduction.....	57
3.3.1.5.Exposition naturelle.....	57
3.3.1.6.Mesures dissuasives .....	58
3.3.1.7.Mesures préventives .....	58
3.3.1.8.Evaluation de l'impact.....	59
3.3.1.9.Potentialité.....	59
3.3.2. Identification des menaces potentielles.....	61

3.3.3. Evaluation des probabilités .....	61
3.3.3.1.Hypothèse de départ .....	61
3.3.3.2.Evaluation de la potentialité .....	62
3.3.3.3.Etat de réduction des risques .....	69
3.3.3.4.Priorisation des scénarios de sinistres .....	72
3.3.3.5.Evaluation des impacts .....	73
3.3.3.6.Sévérité du risque .....	75
3.3.3.7.Choix des menaces à étudier .....	76
3.4.Analyse d’impact sur l’activité .....	77
3.4.1. Interviews BIA .....	77
3.4.2. Identification des activités.....	77
3.4.3. Classification des processus .....	78
3.4.4. Analyse détaillée des processus .....	80
3.4.5. Identification des ressources .....	82
3.4.6. Evaluation des impacts.....	82
3.4.7. Evaluation des objectifs en temps de reprise .....	83
3.4.8. Fonctionnement en mode dégradé.....	84
3.4.9. Synthèse de l’interview BIA .....	84
3.5.Analyse de risque.....	88
3.5.1. Base de connaissance Méhari.....	88
3.5.2. Classification avec Méhari .....	89
3.5.3. Audit de l’existant .....	91
3.5.4. Gravité des scénarios par type d’actif et type d’évènement.....	93
3.5.5. Scénarios retenus.....	94
3.5.6. Choix des plans d’actions.....	96
3.5.6.1.Perte de données applicatives.....	96
3.5.6.2.Perte de données bureautiques partagées .....	97
3.5.6.3.Perte d’archives informatiques.....	97
3.5.6.4.Indisponibilité des services de télécommunication .....	97
3.5.6.5.Indisponibilité du service de réseau étendu.....	98
3.5.6.6.Indisponibilité du réseau local.....	98
3.5.6.7.Indisponibilité de service applicatif .....	98
3.5.6.8.Indisponibilité de service bureautique commun.....	98
3.6.Conception de l’infrastructure optimisée.....	99
3.6.1. Architecture Servers .....	99
3.6.2. Infrastructure de sauvegarde .....	100
3.6.3. Réplication inter sites .....	100
3.7.Implémentation des solutions techniques .....	100
3.7.1. Servers .....	100
3.7.2. Virtualisation .....	101
3.7.2.1.Virtual Center .....	101
3.7.2.2. Gestion des servers ESX .....	102
3.7.3. Configuration SAN .....	103
3.7.4. LUN – Zoning – Masking .....	105
3.7.5. Infrastructure de sauvegarde .....	107

3.7.6. Topologie après refonte.....	111
3.7.7. Réplication inter sites .....	112
3.7.7.1.Stratégie Falconstor et configuration .....	114
3.7.7.2.Etat de basculement.....	115
3.7.7.3.Retour à la normale .....	115
3.8.Elaboration des plans et procédures de continuité.....	117
3.8.1. Maintenance DRP .....	117
3.8.2. Test.....	117
3.8.3. Plan de gestion de crise .....	117
3.8.4. Procédures de sauvegarde .....	117
3.8.5. Plan de continuité et de reprise informatique.....	117
3.9.Retour d'expérience.....	118
3.9.1. Préambule.....	118
3.9.2. Fiches de synthèse.....	118
<b>4. Bilan et alternatives .....</b>	<b>123</b>
4.1.Bilan Projet .....	123
4.1.1. Alternatives .....	123
4.2.Bilan personnel .....	125
<b>Conclusion.....</b>	<b>127</b>
<b>Références .....</b>	<b>128</b>
▪ Bibliographie .....	128
▪ Webographie.....	128
▪ Index des figures.....	129
▪ Index des tableaux .....	130
<b>Annexes-----</b>	<b>131</b>
<b>Table des matières -----</b>	<b>147</b>