Mastère Spécialisé IPISO 2006 :

Ingénierie Production et Infrastructures en Systèmes Ouverts

Thèse professionnelle :

Les Processus et la sécurité en production

Etudiant :	**Tuteur :**
Alexandre Aubry	Sylviane Grange
Entité d'accueil : **/DOE/DOSI/DPROD/DPSIF/ Coordination Transverse**	Stage final du : **07/05/2007 au 10/10/2007**

Remerciement

Je remercie Madame Sylviane Grange responsable du Département Transverse et Responsable National de Processus, mon tuteur pendant mon stage, pour son accompagnement, tant au niveau de l'intégration dans l'équipe que dans l'organisation générale du déroulement du stage.

Son implication permanente, a facilité mon intégration à toutes les phases des différents Projets que j'ai mené ces 5 derniers mois, tout en gardant en mémoire l'objectif de restitution que constitue la rédaction de ma thèse professionnelle.

Je remercie également les équipes techniques d'Emmanuelle Davin et Orane Pitance, particulièrement l'Intégrateur de Pré-Production Christian Rabouin, pour leur aide tout au long de la mission.

Enfin, je tiens à remercier toute l'équipe d'encadrement du Mastère IPISO en particulier Monsieur Jean-Michel FOUVEZ pour leur dévouement et leur confiance au cours de l'année écoulée.

Table des matières

Introduction

Le sujet de stage, objet de cette thèse est « les processus » dans le Système d'information et plus particulièrement le processus de Mise En Production (MEP).

Qu'est ce qu'un « processus » ? A quoi sert-il? Sur quoi s'appuie-t-il ?
Il en sera question tout au long de ce document.

Une macro sur le processus « Mise En Production », sa refonte autour du thème de la sécurité, ainsi que sa mise en place dans la direction de la production du groupe France télécom seront étudiées.

.

1 Présentation de L'entreprise

1.1 Mon entité d'accueil (DOSI)

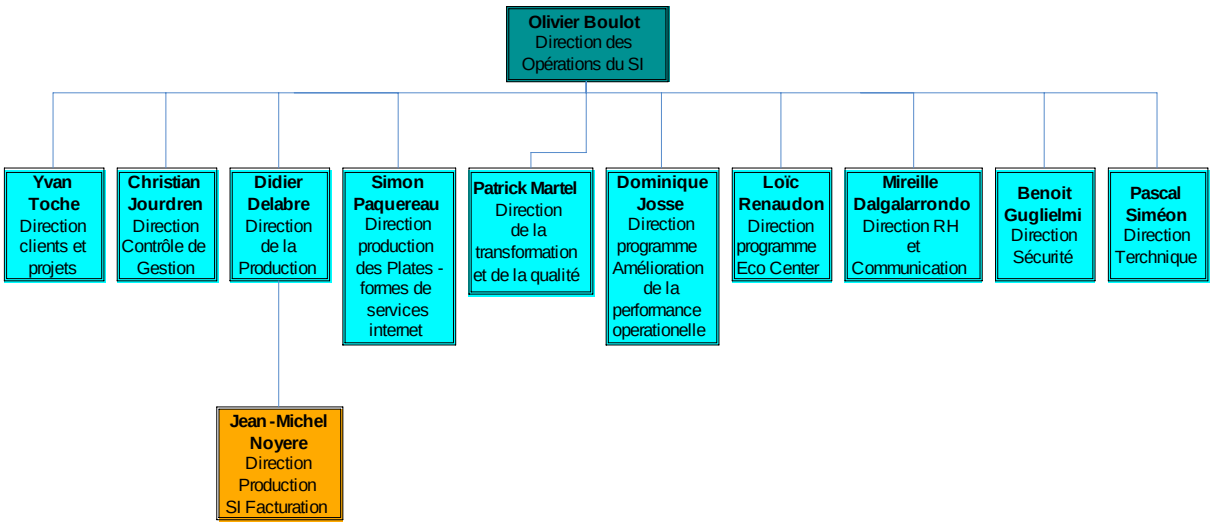
Dans le cadre de ce stage, j'ai intégré la Direction des Opérations du Système d'Information (DOSI).

DOSI est l'entité de France Telecom en charge de piloter la production informatique du groupe.

Ses missions principales sont les suivantes :

- Assurer l'exploitation et la mise en production des applications
- Optimiser et consolider la production informatique du groupe
- Héberger les serveurs, les infrastructures de services et les plates-formes de développement

Organigramme de DOSI



1.2 Présentation des services

Durant ce stage j'ai été affecté au Service de Coordination Transverse qui fait partie de la Direction de Production du SI Facturation. La Direction de la Production du Système d'Information Facturation (DPSIF) est l'une des huit Directions de la Production de DOSI.

1.2.1 Organigramme et Missions de DPSIF

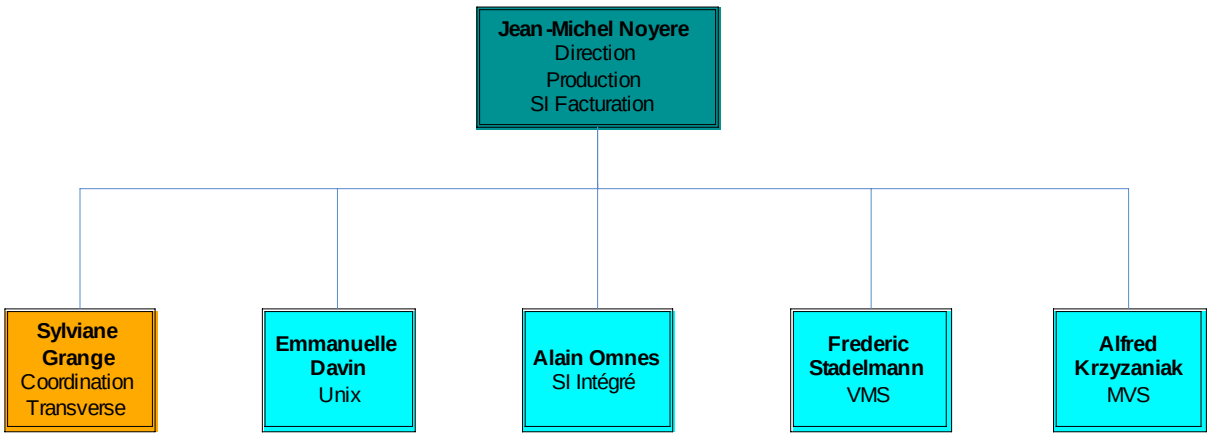
DPSIF est en charge de la production informatique des applications touchant au processus facturation. Elle intègre dans son périmètre les applications de facturation du téléphone fixe, des mobiles et de l'Internet. Elle participe à la stratégie du Groupe France Télécom positionnée comme un opérateur intégré. L'objectif étant de proposer au sein du groupe un large panel de services sur l'ensemble des technologies de téléphonie, appuyé d'une facturation adaptée pour chaque client.

La mission principale de DPSIF est de délivrer le service aux utilisateurs des applications du domaine, dans le respect des contrats de service et aux meilleurs coûts.

Cette mission se décline en trois activités majeures :

- Le pilotage de la production
- Le pilotage des opérations de changement
- Le management de la qualité de service.

Organigramme de DPSIF



1.2.2 L'intégration au sein de la Coordination transverse

Au sein de DPSIF, l'entité Coordination Transverse à en charge :

- la gestion des droits d'accès au système d'information,
- la mise en cohérence des actions sécurité ainsi que des actions de sensibilisation à la Sécurité de l'Information,
- la gestion et la fiabilisation des différents référentiels (applicatif ou non),
- le déploiement de processus Qualité,
- de s'assurer de respecter les différents indicateurs correspondant à la qualité de service via des revues et reporting réguliers,
- la gestion des compétences des Processus et la coordination de tout processus impactant la direction DPSIF,
- la refonte du processus de Mise En Production.

J'ai intégré cette équipe qui se compose de 5 collaborateurs :

- Une responsable de l'entité également responsable national de processus.
- Un responsable qualité des données du S.I.
- Un analyste chargé de la sécurité et des référentiels.
- Deux analystes chargés des reportings et des correspondances locales (SOX, processus).
- Une assistante reporting / référentiels.

Ces collaborateurs sont installés en partie dans les bureaux du site de Daumesnil (Paris 12ème), ainsi que dans des bureaux du bâtiment « Equerre » à Guyancourt (78).

La bonne collaboration entre les différents membres de l'équipe a largement contribué et facilité mon intégration.

1.3 Missions et Objectifs

Dans le cadre de ce stage ; 2 missions principales me sont confiées ;

- La **première** rentre dans le cadre des chantiers de rénovation des livrables de la MEP (Mise En Production) et de l'exploitabilité. Je suis chargé de piloter la refonte des livrables de la sécurité.

Je dois m'appuyer sur la documentation existante et prendre en compte les nouvelles normes de sécurité informatique en vigueur dans le groupe et les intégrer.
Le tout ayant plusieurs objectifs :

- simplifier les formulaires à saisir
- différencier la partie guide et la partie formulaire
- prendre en compte les nouveautés sur la sécurité (projet SISAME, mise en place du dispositif DRP, référentiel 26E, ...)
- éviter les redondances entre les différents documents

Je propose une première esquisse des nouveaux formulaires et guides ainsi que mettre en place et piloter un groupe de travail restreint en m'appuyant sur le résultat de mes travaux.

Lorsque les travaux de ce groupe de travail restreint seront aboutis, ils seront présentés aux CLP (correspondants locaux du processus MEP) pour validation.

L'objectif est de pouvoir communiquer en interne et de faire bénéficier des nouveaux livrables concernant le processus « Mise En Production » au début du Quatrième Trimestre 2007.

- La **seconde** mission est de mettre ceci en pratique, en étant « Chef de Projet Mise En Production (CPMEP)» sur le projet « SANSOM-FE » qui consiste à gérer la migration des plates-formes de production de Windows 2000server à Windows 2003server le tout sans régression de services.

2 Les Processus

2.1 Définition

Le processus est un enchaînement d'activités réalisées avec des moyens et selon des règles, pour générer un produit en sortie destiné à satisfaire les clients en vue d'atteindre un objectif.

Cet enchaînement d'activités comprend un nombre de tâches élémentaires, structurées en procédures. Une tâche correspond à une ou plusieurs actions à réaliser dans un temps fixé, pour laquelle on connaît l'entrée et le résultat attendu. Les tâches indissociables faisant partie d'un processus forment des procédures.

Le processus répond aux questions : QUOI ? POURQUOI ?

On commence à parler en termes de « processus », si après avoir répondu à la question " que faut-il faire ? ", on pose la question " comment faire ? ".

L'approche processus est transversale à l'entreprise et permet d'identifier et de maîtriser les interfaces entre les différents « métiers ».

2.1.1 Les différents types de processus

Il existe différents type de processus :

- Le processus « fonctionnels » appelé également processus « opérationnels » ou « métiers » :

Il représente le cœur de métier de l'entreprise. De l'élaboration à la prise de commande / livraison des produits et services pour les clients.

- Le processus de « supports » :

C'est l'activité de mise à disposition en interne des ressources nécessaires à la réalisation des processus opérationnels : achats de fournitures, RH, comptabilité, etc.

- Le processus de « gouvernance » ou de « pilotage » :

Il s'agit d'élaborer des informations internes permettant le pilotage de l'activité de l'entreprise. On distingue souvent le pilotage opérationnel et le pilotage stratégique.

2.2 Le processus Mise En Production

Le processus « Mise En Production » fait partie de la classe des processus Opérationnels ou processus Métiers.

2.2.1 Les jalons

Un projet est composé de différents « jalon ». Chaque jalon correspond à une partie bien définie du cycle de vie du projet.
Voici un petit tableau correspondant au cycle de vie d'un projet.

Sigle	Intitulé
préJ-1	AVANT ETUDE
J-1	LANCEMENT DE PROJET
J0	DEMARRAGE DU PROJET
J1	ACCORD PRODUIT BUDGET
J1A	ENTREE EN VERIFICATION
J1B	LANCEMENT DE LA MISE EN PLACE PILOTE
J2	DEMARRAGE DE LA GENERALISATION
J2A	TRANSFERT AUX ACTIVITES RECURRENTES
J3	FIN DU PROJET
J4	FIN DE VIE DU PRODUIT

A son initialisation, le projet doit prendre en compte les diverses contraintes que vont entrainer sa mise en production future. Le processus « Mise En Production » est, dès lors, mis en œuvre dès le J0 et certaines documentations relatives à ce processus sont initialisées au J-1.

2.2.2 Les Livrables

Le processus MEP comprend quatre livrables principaux :

- **le cahier d'installation** : Il est mis en œuvre lors de l'installation d'une première version d'une application ou lors d'un changement de version de celle-ci. Ce livrable contient la méthodologie exacte et les pré-requis pour installer l'application.

- **le cahier d'exploitation** : doit permettre pour chaque application de comprendre l'enchaînement des Modules Fonctionnels et techniques de l'application, afin de pouvoir rendre, en toute transparence, le service attendu par l'utilisateur. D'appréhender l'impact d'un dysfonctionnement sur l'utilisateur, d'avoir la maîtrise des priorités fonctionnelles et techniques de façon à pouvoir réagir rapidement en cas d'arrêt imprévu. De référencer éventuellement la nature des informations à remonter aux utilisateurs, le contenu informationnel (messages d'erreur type), ainsi que les destinataires (liste de diffusion) via les acteurs du soutien.

- **le Plan de Travail Commun d'Exploitabilité** : Plan d'action de la mise en œuvre de l'exploitabilité concernant la MOE et l'exploitant. Il représente une vue particulière sur le Plan de Management de Projet concernant cette contribution.

- **le cahier de sécurité** : Description des dispositions pour assurer la disponibilité, l'intégrité, la confidentialité et l'auditabilité de l'exploitation d'une application. La mission qui m'a été confiée est donc de refondre et mettre à jours ce cahier.

D'autres cahiers, extérieurs au processus « Mise En Production » sont tout aussi indispensable au fonctionnement du processus ; à savoir : le Dossier d'Architecture Technique, le Cahier des Exigences Produits et le Cahier des Exigences d'Exploitabilité.

2.3 Le cahier de sécurité

2.3.1 Constat

Le Premier cahier de sécurité a été écrit en septembre 2000. Ce cahier faisait partie des livrables du dossier d'exploitation, ce qui signifie qu'il devait être propre à chaque application.

Ce cahier était sous forme de formulaire où l'on indiquait si l'application répondait bien aux normes d'intégration et de sécurité en vigueur dans la S.I. et sinon, une description succincte de la sécurité mise en œuvre pour l'application était demandée.

Depuis septembre 2000 il n'a été que partiellement complété. Les modifications apportées concernent principalement les différents types de sauvegardes utilisées pour l'applicatif, leurs descriptions (journalière, anti-feu etc…) ainsi que des mini-scénarios de reprise en cas de sinistre sur site.

Avec l'évolution des normes de sécurité dans le S.I (exemple SOX), l'apparition des bonnes pratiques via ITIL, et l'industrialisation des mises en production, ce cahier sous ce format est devenu obsolète.

Il se retrouvait lié à une application tous en parlant de principes généraux de sécurité tel que :

- le type de sauvegarde
- la politique de mot de passe groupe

Le SI ayant également évolué et tout ses processus avec lui on a constaté que le cahier de sécurité reprenait des questions qui étaient également posées dans d'autres documents

2.4 Le Guide de mise en œuvre des services sécurité d'une application en production

Au vu de ce constat, une refonte totale du cahier de sécurité a été demandée par la responsable nationale des processus, afin de prendre en compte les nouvelles exigences de sécurité ainsi que les nouvelles normes au sein du Système d'Information.

Un groupe de travail de 5 personnes a donc été créé afin de mener à bien cette mission.

Ce groupe est composé de :

- Lynda Sidi-Moussa qui appartient à la direction de la sécurité de la production
- Bernard Olivier qui est un des responsables de la sécurité à la Direction du Développement du Système d'Information (DDSI)
- Christian Garcia qui est responsable du pôle exploitabilité au SI Client
- Sylviane Grange qui est la Responsable National de Processus
- Alexandre Aubry qui pilotera ce groupe de travail et qui sera le rédacteur de ce document appartient à la DOSI (Direction des Opérations du Système d'Information)

2.4.1 Première réunion du groupe de travail

Le 25 Juin 2007 eut lieu la première réunion de ce groupe de travail.
Une version réactualisée du cahier de sécurité y a été présentée, sous l'apparence d'un formulaire à questions fermées. Le but étant de faciliter et fluidifier la rédaction de cette documentation pour les chefs de projet qui auront à là fournir lors de chaque mise en production.

Ce formulaire a été rejeté car il est apparu, compte tenu de la mise en place de nouveaux livrables (ex : fiche suiveuse des sauvegardes, cahier de PRA / DRP), ou la rénovation d'autres livrables qui abordent plus concrètement la partie sécurité (Cahier des Exigences Produit – Cahier des Exigences d'Exploitabilité), que le cahier de sécurité ferait doublon.

De plus, il est ressorti de cette réunion que le cahier de sécurité n'était utilisé par personne car on n'arrivait plus à répondre à cette question : « Qui est le destinataire de ce document ? ».

Il a donc été décidé que le cahier de sécurité devait être rédigé dans l'optique d'une utilisation pour les exploitants, par conséquent, qu'un guide autour de la sécurité lors de la mise en production était beaucoup plus adapté, qu'un formulaire supplémentaire à remplir pour chaque nouvelle application à venir en production.

Le groupe a fixé deux objectifs majeurs dans le cadre de la rédaction de ce guide.
Il devra être opérationnel et il devra répondre aux exigences concernant le « DICA » (Disponibilité, Intégrité, Confidentialité, Auditabilité).

2.5 Les problématiques soulevées dans le guide

2.5.1 Les critères de sécurité

Une sécurité informatique efficace repose sur 3 critères principaux :

- **Intégrité :** propriété d'exactitude et de complétude des *informations* et des *fonctions* de l'information traitée lors du déroulement des différents processus.

- **Confidentialité :** propriété d'une *information* ou d'une *ressource* de n'être accessible qu'aux utilisateurs autorisés (création, diffusion, sauvegarde, archivage, destruction).

- **Disponibilité :** propriété de disposer dans des conditions de délais définis des *informations* et des *fonctions*.

- **Auditabilité :** garantie de la maîtrise complète et permanente sur le système, et en particulier de pouvoir retracer tous les événements au cours d'une certaine période.

2.5.2 Les exigences de sécurité

La Maitrise d'ouvrage (MOA) doit exprimer avec une certaine hiérarchisation les priorités de sécurité (fiabilité / indisponibilité / intégrité / confidentialité / traçabilité).

La Maitrise d'œuvre (MOE) récupère ces demandes et les traduit techniquement à travers les documents suivants:

- le DAT & le plan de nommage
- le cahier des exigences produit
- les contrats d'interface

Les objectifs de sécurité sont couverts par la déclinaison d'exigences techniques et organisationnelles.

La MOA a exprimé ces exigences sécurité à travers le cahier des exigences produits. Cependant, l'exploitant a ces propres exigences de sécurité. Il les développe dans le cahier des exigences d'exploitabilité.

2.5.3 Détermination des besoins en disponibilité

La MOA devra :

- présenter les fonctions Métiers vitales.
- définir la notion d'indisponibilité des services qu'elle propose.
- analyser l'impact Métier de l'interruption du Service.
- formuler les délais Métiers acceptables pour l'interruption de Service et le fonctionnement en dégradé.
- déterminer les jours et heures pour la fourniture du service (ex : 8H-18H 5J/7, 24H/24 7J/7)
- présenter le calendrier des différentes périodes de travail Métiers (périodes critiques : T4, fin de mois, ..).
- exprimer des besoins de sécurité spécifiques.

De plus, elle devra définir la stratégie de sauvegarde/restauration pour l'application en indiquant la périodicité :

- des sauvegardes des données (journalière, hebdomadaire, …),
- des sauvegardes applicatives (journalière, hebdomadaire, mensuelle,…),
- des sauvegardes systèmes (hebdomadaire, mensuelle, …),

ainsi que la durée de rétention des sauvegardes.

Elle devra définir le besoin et la périodicité des :

- sauvegardes anti-feu,
- archives administratives et légales (avec durée de rétention).

2.5.4 Exigences concernant la continuité de service

A travers sa demande de continuité de service, la MOA doit déterminer l'impact et évaluer les risques d'une interruption métier.

Elle devra définir les mesures permettant de réduire les risques et les options de reprise pour supporter les besoins métiers en s'appuyant sur la gestion de la disponibilité des services.

Elle demandera la mise en place de technologies permettant de diminuer les risques (redondance du matériel, politique de sauvegarde/restauration, etc.).

elle devra notamment définir l'utilité de la mise en place d'un Plan de Reprise Applicatif (PRA).

Le périmètre du PRA est généralement celui d'une application.

L'objectif du PRA est de détailler l'ensemble des éléments organisationnels, techniques et fonctionnels permettant de décider et exécuter jusqu'à son terme la reprise de l'application considérée sur sa plate-forme de secours, située dans un datacenter différent de celui habituel de production, suite à un incident ou un sinistre grave.
Cette exigence sera reprise dans le SLA.

2.5.5 Service Level Agreement (SLA)

Définition : contrat définissant les obligations d'un hébergeur de service vis-à-vis d'un fournisseur de service en matière de niveau de qualité de service.
Cette qualité doit être mesurée selon des critères objectifs acceptés par les deux parties.
Ex : temps de rétablissement du service en cas d'incident.

Le SLA définit :

- le niveau de prestation des sauvegardes (système, applications, données) mis en œuvre,
- la fréquence de tests de restauration et la durée de rétention,
- la perte de données maximale admise ➔ **RPO**,
- la durée maximale d'indisponibilité totale de l'application ➔ **RTO**,
- le délai de restauration de l'application sur sinistre ➔ **DRAS**.

De plus, le SLA décline la stratégie mise en œuvre pour assurer la continuité de service :

- Soit un Plan de Reprise Applicatif (PRA) est mis en œuvre et ce plan s'appuie sur :
  - Sur une architecture répartie entre plusieurs sites (au moins deux) et les procédures d'exploitation associées, le tout permettant d'assurer une continuité du fonctionnement de l'application en cas de sinistre d'un des sites.
  - Sur une ou plusieurs plates-formes de secours identifiées avec leurs procédures associées, pour une reprise de l'application sur un site distant en cas de sinistre de l'application sur le site de production.
- Soit seule une externalisation des données de l'application est en place (sans plate-forme de secours distante).
- Soit l'exploitant n'a aucun engagement sur une reprise des données et de l'application.

2.5.6 Exigences d'intégrité

De manière générale, l'intégrité des données désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.

L'intégrité des données comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité.

Pour l'exploitant, la réponse aux exigences d'intégrité s'appuie sur la politique de sauvegardes et la politique des contrôles d'accès.

2.5.7 Exigences de confidentialité

L'objectif de la confidentialité est la préservation du secret et du savoir-faire.

C'est une exigence en vertu de laquelle une information est divulguée, traitée et mise à la disposition des seules personnes ou entités autorisées, selon les modalités établies.

La MOA devra définir les différents profils des utilisateurs et associer à chacun leurs droits

2.5.8 Exigences d'exploitabilité

Pour répondre à la demande d'une exploitation sécurisée, l'exploitant exprimera des exigences sur :

- **La sécurité des échanges** : le transfert de données entre applications devra se faire selon des procédures normalisées. La sécurité devra intervenir à travers le réseau et le protocole d'échange, éventuellement la cryptographie.

- **La traçabilité et l'auditabilité** : si la traçabilité permet de qualifier la possibilité de reconstituer la chronologie de tout type d'événements et de contribuer ainsi à apporter des réponses à tout type d'incidents, l'auditabilité doit permettre de détecter les vulnérabilités particulières.

2.5.9 Activités de contrôle SOX

Deux lois sur la sécurité financière ont été promulguées :

- la loi Sarbanes-Oxley Act, aux USA, en Août 2002

Cette loi est applicable aux sociétés cotées aux USA et s'applique donc à France Télécom

- La loi de Sécurité Financière, En France, en Août 2003

Objectif : conduire les entreprises vers une meilleure gouvernance d'entreprise

2.6 Les réponses apportées par le guide

2.6.1 Disponibilité - Continuité de Service

Les outils et infrastructures de sauvegarde sont indispensables à la sécurité des données du SI. Ils permettent de restaurer un environnement de travail utilisateur en cas de perte de données utilisateurs ou crash serveur. Ils interviennent notamment dans le cadre d'un PRA (Plan de Reprise d'Activité)

2.6.1.1 Solution mise en place pour les sauvegardes

Fiche suiveuse : initialisé au J0, elle est le document de base pour les exploitants, elle regroupe les informations concernant les différentes stratégies de sauvegardes identifiées dans les exigences exprimées par la MOA.
Elle est instruite par le CPMEP du projet. Elle est l'outil de dialogue entre les équipes opérationnelles qui mettent en œuvre le plan de sauvegarde défini.

La fiche suiveuse s'appuiera sur le DAT, et éventuellement sur un cahier de sauvegardes si la stratégie de sauvegarde n'était pas décrite dans le DAT.

Les solutions mises en place par le groupe France Télécom s'appuie sur les technologies suivantes :

Centricstor ➔ C'est une solution de virtualisation de sauvegarde. Elle permet de virtualiser les librairies de sauvegarde et de les partager entre différents types de serveurs et différents logiciels de sauvegarde.

Dans l'état actuel de la législation et de la technologie, seuls **les disques WORM** (W*rite Once Read Many*) de type DON ou UDO répondent totalement à toutes les obligations de protection et de non-réinscription des informations.
Il existe actuellement des solutions WORM sur disque dur en cours de certification auprès des organismes normalisateurs.

RMAN (Recovery Manager) ➔ est un des utilitaires standards de la base de données Oracle. Il permet aux DBA de gérer les opérations de sauvegarde/restauration

Il offre la possibilité :

- De réaliser des sauvegardes globales de la base. C'est un type de sauvegarde nommé « **COMPLET** » (ou « **FULL** ») : On sauvegarde tous les blocs.
- De réaliser des sauvegardes incrémentielles **différentielles** : permet de sauvegarder uniquement les blocs modifiés depuis la précédente sauvegarde de niveau n ou inférieur.
- De s'interfacer avec un outil de sauvegarde externe (gestionnaire de médias : netbackup).
- D'effectuer des restaurations globales ou partielles.

- De gérer les périodes de conservation des sauvegardes.
- De dupliquer une base de données de manière simple.
- De vérifier les sauvegardes effectuées en termes de corruption et ne corrompt pas les bases qu'il sauvegarde (contrairement à la copie de fichiers de données sans positionner les tablespaces en mode backup).

NetBackup (NBU) ➔ Netbackup est un logiciel de sauvegarde "applicative". Il est basé sur une architecture client/serveur et assure la totalité des fonctions de sauvegarde/restauration, d'archivage des données dans un environnement distribué. Son architecture est basée sur trois niveaux : Le serveur "principal" ou Master, les serveurs de sauvegarde ou slaves, les clients.

NetBackup est architecturé autour d'une structure à 3 niveaux qui distingue :

- le serveur principal ou "Master Server", sur une station d'administration, qui permet la mise en place des procédures de sauvegarde automatique et de gestion des médias, ainsi que la supervision des opérations,
- des serveurs de sauvegarde ou "Media Server" définis en différents points du réseau et qui se partagent la charge de la sauvegarde proprement dite et le contrôle des périphériques de stockage,
- les clients, qui sont en charge, sur les stations clientes, des fichiers, des répertoires, des bases de données et de toutes informations résidantes (incluant les "raw partitions" et autres fichiers spéciaux) nécessitant d'être prise en compte par les opérations de sauvegarde.

L'architecture à 3 niveaux de NetBackup permet de gérer des sites distants, en préservant la cohérence de l'architecture.

2.6.2 Réponse reprise de l'applicatif sur sinistre

Pour permettre de tenir l'objectif d'une continuité de service, la mise en œuvre d'un Plan de Reprise Applicatif (PRA) s'appuie sur plusieurs solutions :

2.6.2.1 La répartition de charge

Cette solution permet de garantir un niveau optimal de qualité de service à l'utilisateur final.

Le partage de charge permet aussi de répondre aux exigences de « haute disponibilité » ainsi que d'accroitre les performances et la scalabilité d'une application.

Le partage de charge peut-être local (sur le même data center) ou multi-site. Seul le partage de charge multi-site répond au besoin de PRA.

2.6.2.2 La réplication de base de données

La réplication de base de données s'appuie sur un serveur de back up.

La réplication des bases de données s'effectue en mode Synchrone ou Asynchrone.

Lors d'une réplication, l'utilisation de la base de données sera opérationnelle.

Il est à noter que le "load balancing" (transfert de charge) s'appuie sur le mécanisme de réplication. En cas de surcharge d'un serveur, on peut être amené à dérouter certains utilisateurs vers des serveurs secondaires dont la base aura été répliquée.

2.6.2.3 La restauration des données

La solution mise en œuvre peut s'appuyer sur la restauration des données, à partir de la dernière sauvegarde, sur un serveur de back up placé dans un data center distant.

La Capacité disponible sur le site de secours est une Capacité dormante. En temps normal, elle peut être utilisée à des activités de pré-production ou d'intégration, mais ces activités seront immédiatement arrêtées en cas de sinistre et les ressources réquisitionnées.

2.6.3 Situation de sinistre d'un data center : Mise en œuvre du DRP

Le DRP (Disaster Recovery Plan) est le dispositif mis en place pour maintenir les activités métiers critiques en cas situation de sinistre (perte/indisponibilité de toute ou partie d'un site).

Pour supporter le redémarrage des processus métiers critiques dans les délais prévus, il s'appuie sur une stratégie d'équilibre :

- le coût des mesures de réduction des risques,
- les scénarios de reprise

Une cellule de crise doit définir les priorités de remise en route des serveurs/applications vitales à l'entreprise.

C'est un dispositif principalement organisationnel et décisionnel. On trouve dans ce document :

- les éléments qui permettent de monter une cellule de crise avec les personnes concernées par l'incident majeur,
- les éléments permettant de piloter la crise de manière centralisée : inventaire et référentiels des applications et serveurs localisés dans le data center sinistré, caractéristiques du data center (surface, salles, …) et la cartographie des salles en fonction de leurs usages : (SI FT, plateformes de service, …).

En ce qui concerne la partie applicative, le DRP doit s'appuyer sur les documents de PRA lorsqu'ils existent.

2.6.4 Confidentialité

A travers la confidentialité, on doit pouvoir associer de manière plus ou moins forte un identifiant et une personne.

La réponse se fera à travers la politique de gestion des habilitations dans le S.I du Groupe France Telecom (note interne **GITNS004) :**

Contrôle d'accès des utilisateurs aux applications : Une note interne (La 2007/S20 écrite par ROSI/ITNPS/TAS) énonce, dans le cadre SOX, les exigences sécurité pour couvrir le risque d'identification/authentification.

Ces exigences doivent se généraliser sur les applications hors du périmètre SOX.

2.6.4.1 Pour les applications passant par le GASSI

GASSI est un Gestionnaire d'Accès Sécurisé interne au Système d'Information :
C'est un produit permettant au travers d'une fonction **SSO** (Single Sign On), la gestion centralisée des droits des utilisateurs pour leur accès à toutes les applications du SI. Le **SSO** est une fonction permettant de disposer d'une identification unique, quelque soit le service applicatif.

GASSI permet :

- L'accès aux applications via une infrastructure de rebond sécurisé.
- L'authentification et l'autorisation d'accès à chaque tentative via l'infrastructure sécurisée, par la vérification d'une base d'habilitation où sont définis les profils et les droits associés à l'exploitant.

2.6.4.2 Pour les applications hors GASSI

Les principes de sécurisation des accès devront être documentés. Ils devront notamment s'appuyer sur les règles suivantes :

- Un mécanisme de vérification d'identité de l'utilisateur (login/MdP/certificats).
- Une politique de mot de passe compris entre 8 et 12 caractères et contenant
  - au moins un chiffre,
  - une lettre majuscule,
  - une lettre minuscule,
  - un caractère spécial (? $ …),
  - une durée de vie limitée (12mois) et une historisation des 6 derniers mois,
  - un verrouillage du compte après 4 tentatives de connexion.
- Les logs de connexion des applications hors Gassi devront être sauvegardés pour la traçabilité/auditabilité.

2.6.5 Contrôle d'accès aux serveurs en exploitation

2.6.5.1 Outils de contrôle d'accès

On appelle contrôle d'accès le fait de n'autoriser l'accès aux informations et aux ressources qu'à ceux qui en ont besoin.

La MOE respectera les **règles de sécurité** du groupe FranceTélécom

- L'accès des exploitants aux serveurs en production est réalisé via une infrastructure de rebond sécurisé (AD et TDIMG).

- L'authentification et l'autorisation d'accès sont réalisées à chaque tentative via l'infrastructure sécurisée par la vérification d'une base d'habilitation (AD et TDIMG) où sont définis les profils et les droits associés à l'exploitant.

AD ➔ Active Directory : est un annuaire au sens informatique et technique, qui permet de gérer les ressources du réseau : données utilisateur, imprimantes, serveurs, bases de données, groupe, ordinateurs et stratégies de sécurité. Les administrateurs peuvent contrôler leurs utilisations grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation des accès aux ressources répertoriés.

TDIMG (Télé Diagnostique et télé Intervention en Mode Graphique) : est une infrastructure de rebond pour accéder aux serveurs de production. Cela permet de sécuriser les accès au système des serveurs pour les exploitants du SI.

Cette Technologie fait partie du Projet **SISAME** (Sécurisation de l'Accès aux Machines pour les Exploitants).
Le projet SISAME ne couvre pas les accès métiers aux applications, ces accès relevant du GASSI.

2.6.5.2 Préconisations

- Ne pas utiliser le compte « root » pour des tâches d'exploitation.
- Utilisation de connections de type SSH pour se connecter sur les serveurs.
- Faire un audit de sécurité. L'objectif est d'être en conformité avec les règles données par le RSSI (Règles de Sécurité du Système d'Information). Toutes les informations relatives au RSSI peuvent se trouver sur l'intranet de l'entreprise.
- Faire un audit de vulnérabilité réseau.
- Remplir un formulaire officiel pour répertorier les différents utilisateurs des Bases de Données. Ce formulaire est actuellement en cours de validation par la Direction de la Sécurité de la Production.

2.6.6 Exploitabilité

2.6.6.1 La Traçabilité

La gestion de la traçabilité constitue un **point critique** des recommandations SOX. En effet, cette réglementation nécessite une parfaite maîtrise de tous les flux informatiques de l'entreprise.

On s'appuiera sur l'**activité de contrôle (T5AC8)** pour définir les contours des exigences de traçabilité pour l'exploitation :

« Les travaux différés ou non font l'objet d'un ordonnancement (planification). Un compte-rendu d'exécution en collecte les traces. Ces traitements sont contrôlés par le domaine de production concerné. Pour chaque famille de pratique homogène (UNIX, MVS, VMS, AS400), un mode opératoire fournit les modalités des contrôles à réaliser. Les erreurs de batch donnent lieu à une signalisation tracée dans l'outil de gestion des incidents ».

La maîtrise des flux informatiques s'appuie sur la gestion des logs.

L'abondance et la corrélation de ces informations permettent d'optimiser les systèmes d'information et de retrouver les sources des pannes informatiques.

Cependant, ces données indispensables aux administrateurs deviennent de plus en plus nombreuses sans être forcément pertinentes. De ce fait, sans un traitement automatisé efficace, certaines alertes critiques se retrouvent inondées sous **la masse de faux positifs.**

Les journaux d'évènements sont des fichiers contenant des informations brutes sur les activités d'un réseau, d'un service ou d'une application. Les contenus des logs sont **très variés** car ils rassemblent aussi bien des opérations de fonctionnement normal que des erreurs survenues ou des tentatives d'utilisation frauduleuse.

Ces fichiers vont permettre aux administrateurs d'analyser les utilisations des différentes ressources du parc informatique afin de sécuriser, de fiabiliser et d'optimiser le système d'information. En outre, la journalisation permet d'offrir une garantie juridique lorsque la responsabilité de l'entreprise est engagée ou lorsqu'un individu malveillant s'introduit au sein de son réseau.

Les **principaux enjeux de la gestion des logs** sont donc :

- la validation de la **politique de sécurité**
- l'**optimisation des coûts** d'exploitation
- l'aide à la **gestion des risques**
- la **protection juridique**

Afin de lutter contre l'utilisation frauduleuse ou abusive des ressources informatiques, il est courant de journaliser toutes les connexions aux services et aux applications.

2.6.6.2 L'auditabilité

A travers l'auditabilité, une preuve de délivrance de l'information de façon authentifiée et non-répudiée est disponible, la non répudiation, permettant de garantir qu'une transaction ne peut être niée ou cachée.

La démarche d'auditabilité permet d'attribuer aux systèmes auditables (et à leur sécurité) un certain niveau de confiance.

Par la politique de sécurité mise en place, nous pouvons garantir auprès des auditeurs SOX :

- la disponibilité : (mise en œuvre d'une politique de sauvegardes, PRA, …),
- le contrôle des sauvegardes via des tests de restauration et la mise œuvre de la fiche suiveuse,
- le suivi des connexions des utilisateurs en conservant toutes les traces,
- l'authentification et contrôle d'accès, à travers notamment le projet SISAME avec pour couverture technique le GASSI et TDIMG,
- la confidentialité définie dans la note interne GITNS004.

2.6.6.3 Audits de sécurité interne

Un des acteurs de la mise en production (MOA, MOE, CPMEP), peut être à l'initiative d'une demande d'audit sécurité sur leur application.

Ces audits peuvent concerner le réseau, les systèmes (Unix, Linux, Windows) ainsi qu'Oracle.
Ils peuvent avoir lieu lorsque l'application est en production (fréquence et cible à définir).

Pour plus d'information concernant la réalisation d'audit interne, le « Guide de réalisation des audits interne de sécurité » référencer G 005 108 est à disposition sur le référentiel documentaire de l'entreprise.

2.6.7 Sécurité des échanges

Cela répond aux exigences d'intégrité et de confidentialité

Il y a diverses préconisations comme :
- ne pas utiliser le protocole FTP ni RCP pour les transferts de fichiers,
- préconisation de CFT pour les transferts de fichiers,
- utilisation de moyen de cryptage pour les données sensibles lors de leurs transferts.

Cryptage ➔ processus transformant l'information dans un format secret pour éviter que des personnes non autorisées puissent l'utiliser si elles arrivaient à s'en emparer.

Ensuite, il y a une politique concernant les transferts de fichiers qui a été mise en place ainsi que des règles spécifiques pour l'utilisation et le paramétrage du logiciel CFT. Tout ceci a été édicté dans des documents disponibles sur le référentiel documentaire de l'entreprise.

2.6.8 Les livrables autour du guide de mise en œuvre des services de sécurité

Voici un tableau regroupant les différents livrables faisant partie du processus « Mise En Production » ainsi que tous ceux qui ont un lien direct avec la sécurité en production.

Livrables		Responsable et acteurs	Pour qui	Quand
DAT (avec déclinaison des exigences de sécurité)	O*	MOE – Architectes	MOE, Exploitants, CVAT MOA	J0
Cahier des Exigences Produits	O	MOA avec aide MOE	MOE, Exploitants	J0
Cahier des Exigences d'Exploitabilité	O	Exploitant	MOE, MOA	J0
Cahier de sauvegardes	F**	MOE	Exploitants	J0
Fiche Suiveuse (caractéristiques des sauvegardes)	O	CPMEP Contributeur Équipes Sauvegardes	Exploitants, équipes sauvegardes	J0
Rapport d'audit	F	MOA Porteurs DSSI MOA Acteur CNSSI	Exploitant, MOA, MOE, CVAT	J1-B
CR tests de restauration	O	MOE	MOE Processus qualification, processus exploitabilité	J1-B
Cahier d'Exploitation, Cahier de Supervision, Cahier des Flux	O	MOE	Exploitants	J1-B

* : O➔ Obligatoire
**: F➔ Facultatif

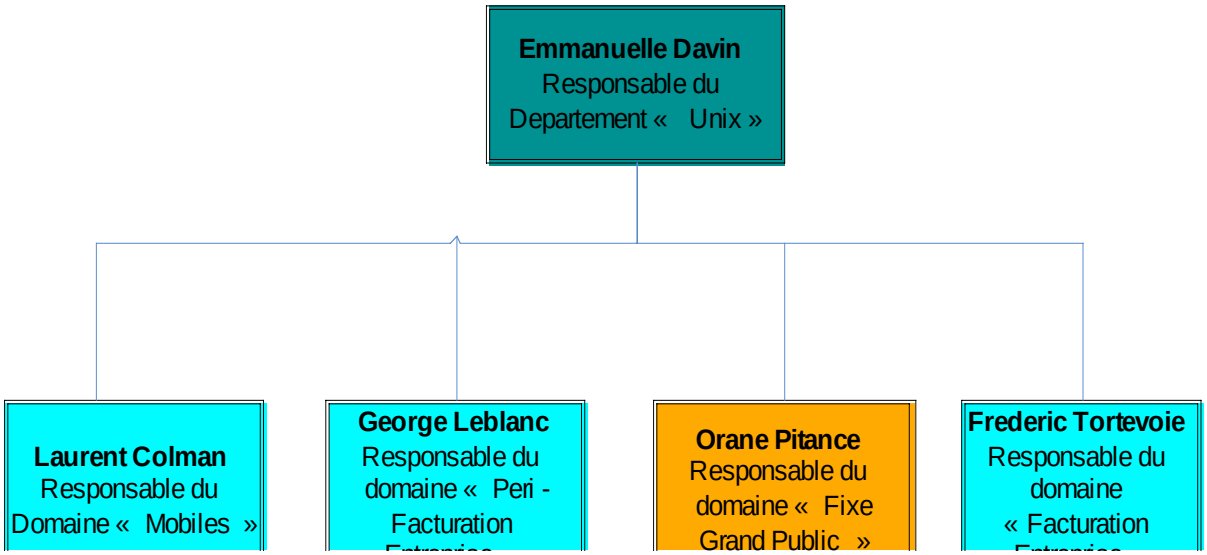
2.7 Apport personnel par rapports à la formation

L'étude durant mon cursus théorique de :
- La manière de « conduire » le changement dans un S.I.
- Les relations Maîtrise d'Ouvrage, Maîtrise D'Œuvre et Production dans un S.I.
- Les normes, (ITIL, etc…).

Ainsi que mon experience professionnelle (intégrateur de production), m'ont permit d'avoir un regard périphérique sur les travaux à mener, ce qui m'a aidé à mener à bien ma mission.

3 Projet technique « Sansom »

3.1 Organigramme et Missions de l'équipe « Unix »



Chaque équipe est chargée de faire la mise en production et de faire le soutien aux exploitants pour les applications de son domaine.

3.1.1 L'intégration au sein de l'entité « Unix »

Au sein de DPSIF, l'entité Unix n'a que pour seule Maîtrise d'œuvre le SI Facturation et à donc en charge :

- La mise en production des applications Orange Unix
- La mise en production des applications Orange Windows
- Le soutien Applicatif de Niveau 2 de ces mêmes applications

Toutes ces applications ont pour Maitrise d'œuvre l'entité SIFAC (SI Facturation).

J'ai principalement eut pour interlocuteur l'équipe d'Orane Pitance et plus particulièrement l'intégrateur de production Christian Rabouin.

L'équipe d'Orane Pitance se compose de 4 collaborateurs :

- Un intégrateur de pré-production
- Un Gestionnaire d'application
- Deux intégrateurs d'exploitation

Ces collaborateurs sont tous installés dans des bureaux du bâtiment « Equerre » à Guyancourt (78).

3.2 Contexte

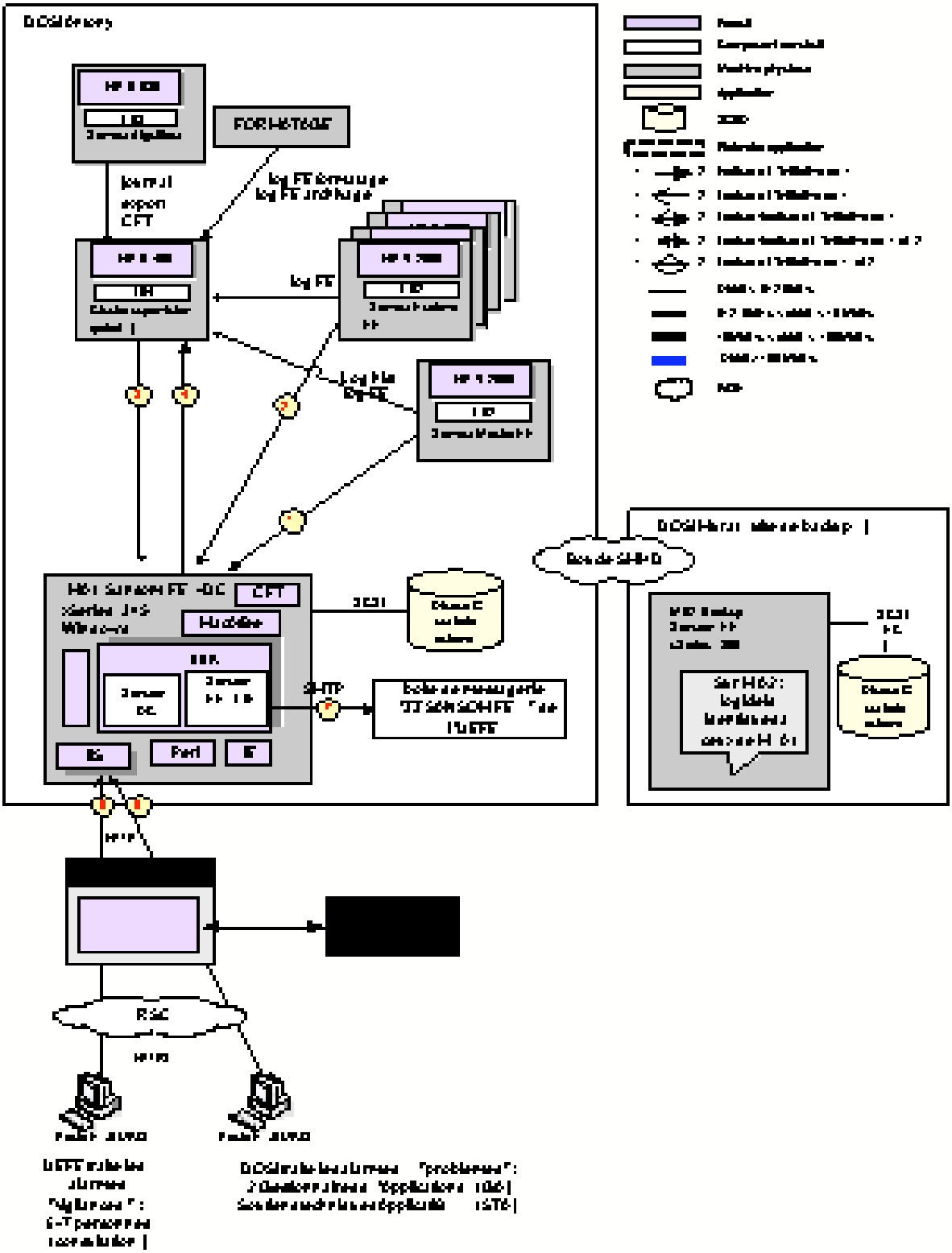
Sansom ➔ **S**urveiller pour **AN**ticiper par la **S**upervision **O**rientée **M**étier

L'application « SANSOM FE », actuellement en production dans sa version G4R0, concerne la supervision de la chaîne de valorisation des détails de communication de FE, à partir du progiciel de contrôle de processus métier Business Bridge (BBR) de la société SYSTAR.

Cette supervision de la chaîne FE doit, en temps réel :

- Fiabiliser le suivi des flux,
- Surveiller la complétude des DC pour les TOP facturation,
- Automatiser la production des compteurs d'anomalies et les surveiller,
- Alarmer les personnes désignées en cas de détection d'anomalies et gérer les alarmes,
- Produire des indicateurs décomposés en différentes classes :
    - Indicateurs d'exhaustivité,
    - Indicateurs de ponctualité,
    - Indicateurs de cohérence,
    - Indicateurs de vraisemblance,
    - Indicateurs de fluidité.

3.3 Architecture Technique



3.4 Evolution technique

Cette version G4R1 correspond à une évolution technique de l'application du fait de la fin du support de Windows 2000server par Microsoft fin mars 2007. Le système d'exploitation évolue vers Windows 2003server.

3.5 Les processus Sécurité dans le projet

3.5.1.1 Fiabilité de service

- **Fail over**

Il existe un serveur de backup identique techniquement au serveur de production. La bascule de fail over se fera manuellement en cas de besoin. Cette bascule engagerait les actions suivantes :

1. Restauration des données à J-1,
2. Adaptation réseau,
3. Restauration et Validation du paramétrage applicatif et redémarrage,
4. Réception des flux CFT qui n'avaient pas pu être réceptionnés.

- **Montée en puissance par introduction d'une architecture à « étage » :**

Un premier serveur peut être dédié à l'analyse d'un ou plusieurs indicateurs demandant un traitement important pour la corrélation et le calcul d'impact. Celui-ci enregistre le résultat de l'analyse dans un fichier log qui va servir de Data sources à un serveur central d'analyse centralisant la remontée de tous les Data Sources et ainsi libéré d'un trop lourd traitement.

3.5.1.2 Réponses aux critères de Sécurité

L'intégrité est assurée par la limitation des accès au serveur aux seuls administrateurs en modification du progiciel. Les utilisateurs de la supervision n'y accèdent que pour de la consultation.
Le progiciel offre des dispositifs de redémarrage sur incidents au travers de la gestion d'un journal.

Le niveau de confidentialité est assuré par Business Bridge(BBR) dans sa version 3.5 qui s'appuie sur la politique de sécurité de Windows, gère ses propres utilisateurs. La solution ne dispose pas d'ouverture sur Internet, ni sur Extranet actuellement. Seuls les administrateurs accèdent au serveur BBR en modification (2 personnes).

Le niveau de disponibilité est assuré ainsi que le niveau de sensibilité exigé par la présence d'un serveur assurant un backup, pré-configuré avec deux disques de boot chacun supportant une version différente de l'OS (mutualisation du backup de Sansom DC - FE et Sansom éditique). Seul un backup de serveur est assuré et non un secours sur destruction de site (application jugée non prioritaire).
Les disques fonctionnent en miroir. Le backup permet un redémarrage dans les 4 heures après décision de bascule (restauration des données, adaptation réseau, boot du serveur de backup sur le bon OS, validation du paramétrage applicatif et redémarrage).

3.6 Exigences de fiabilité de service

Critères liés aux niveaux de service	
Ouverture de service	24/24 7/7
Nombre d'arrêts de service tolérés	1 fois par jour pour permettre la sauvegarde des données. La durée prévisible des sauvegardes est estimée à 1 Heure au travers d'une mise en œuvre de NetBackup.
Fenêtre d'exploitation demandée	À partir de 20h00.
RTO « begin » (Recovery Time Objective sur incident « bénin ») = DMIA incident mineur **Durée maximale d'interruption admise ET type de bascule**	Le temps d'indisponibilité maximum d'affilé toléré est de **4 heures/mois**. Le nombre total d'heures d'indisponibilité tolérée est de **4 heures / utilisateur / an**. Le nombre maximum d'indisponibilités par mois est de **2**. Bascule manuelle de M1 sur M2. Pas de mode dégradé.
RPO « begin » (Recovery Point Objective sur incident « bénin ») = Perte de Données max. admissible sur incident mineur	Aucune perte de données n'est tolérée. Cette disponibilité est assurée par des disques en miroir.
RTO (Recovery Time Objective) = DMIA sur sinistre **Durée maximale d'interruption admise ET plan de reprise**	Désastre de site non couvert.
RPO (Recovery Point Objective sur sinistre) =Perte de Données max. admissible – Désastre site	
Demandes exceptionnelles	La plage disponible pour les opérations de changement de versions, maintenance, s'inscrit dans un creux d'activités à superviser et par déport de la charge sur le serveur dormant, les actions de maintenance sont réalisées sur intervention de l'administrateur Windows.

3.7 Solutions et moyens de Sécurité (Accès et Fonctionnement)

Fonctions de sécurité logique	Mesures	Générique, spécifique, possible
Intégrité des données	Garantie de la non altération des données	réalisées par BusinessBridge ainsi seules les vues pour lesquelles il est habilité sont visibles à un utilisateur. D'autre part, aucune manipulation directe des données du système n'est possible au travers d'IHM.
Traçabilité	Traçabilité applicative et système d'action d'utilisateurs	
Imputabilité	Exploitabilité des traces : Attribuer, avec le niveau de confiance exigé, une action sur une information ou une ressource à un utilisateur déterminé	systématiquement réalisés par Business Bridge dans un journal dédié. Ceci permet à l'administrateur de tracer les tentatives d'accès frauduleux au système.
Non répudiation	Certification d'émission et réception	
Confidentialité des données	Confidentialité de l'information (création, diffusion, sauvegarde, archivage, destruction)	assuré par Business Bridge dans sa version 3.5 qui s'appuie sur la politique de sécurité de Windows, gère ses propres utilisateurs.
Sécurité des échanges	Pour l'ensemble des flux applicatifs, y compris échanges avec les utilisateurs : Identification/authentification des partenaires, Intégrité, disponibilité de l'échange, confidentialité de l'échange	politique de sécurité de Windows La solution ne dispose pas d'ouverture sur Internet, ni sur Extranet actuellement. Seul les administrateurs accèdent au serveur BBR en modification 2 personnes.
Identification / Authentification	Identification et authentification de tous les utilisateurs Règle sur les mots de passe (attribution, modification…)	L'utilisateur a droit à trois tentatives (nombre paramétrable) pour fournir son mot de passe. Passées ces trois tentatives, l'accès de l'utilisateur est temporairement ou définitivement bloqué (dans ce cas, il doit être ré-autorisé par l'administrateur qui réinitialise son mot de passe). Par ailleurs, l'utilisateur doit obligatoirement changer son mot de passe si celui-ci date de plus de trois mois.
Contrôle d'accès	Capacité de restreindre l'accès à une information ou à une ressource aux utilisateurs légitimes par des contrôles appropriés exercés sur leurs droits	Business Bridge dans sa version 3.5 s'appuie sur la politique de sécurité de Windows et gère ses propres utilisateurs.

3.8 Cycle de vie du projet

3.8.1 Le planning

Jalons	Dates prévisionnelles	Actions Principales
J0	14 Mai 2007	Initialisation du projet
J1A	26 Juin 2007	la MOE fourni les livrables applicatif
J1B	03 Octobre 2007	Mise en production du serveur IBSAMS02*
J2	06 Novembre 2007	Mise en production du serveur PNSAMS02*
J2A	12 Novembre 2007	PV de recette d'exploitabilité et vérifications des conformités des règles de sécurité en production

*

- IBSAMS02 est le serveur de back-up de l'application SANSOM-FE
- PNSAMS02 est le serveur de production de l'application SANSOM-FE

3.8.2 Le déroulement du projet

Le projet consiste à migrer 2 serveurs de Windows 2000server vers Windows 2003server.
L'un des serveurs étant en production et le second en pré-production.

On va détailler les différentes phases qui vont nous permettre de réaliser cette migration, en limitant au minimum l'indisponibilité vis-à-vis du client, mais aussi en prenant en compte les règles de sécurité de Mise en Production.

Mon rôle, dans cette opération, est d'être le chef de projet mise en production (CPMEP).

3.8.3 Entre le J0 et le J1A

Lors de cette première phase est prononcée l'initialisation du projet.
Pour le projet « SANSOM-FE » ce fut fait à la date du 14 Mai 2007.

Les premiers éléments du projet, comme le plan de nommage, sont déjà définis.
Il est demandé aux diverses équipes de le respecter.

Très rapidement l'exploitation fourni le Cahier des Exigences d'Exploitabilité à la Maitrise d'œuvre.
La maitrise d'œuvre retourne ce cahier au Chef de Projet MEP dans les plus bref délais, avec ou non des annotations à l'intention de l'exploitation.
Une fois que les deux entités sont parvenues à un accord, le cahier des exigences d'exploitabilité est validé par la maîtrise d'œuvre.
Dans notre cas il fut confirmé au 30 Mai 2007.

En tant que CPMEP, j'ai dû prendre contact avec tous les interlocuteurs susceptibles de travailler sur ce projet. Les équipes chargées de la sauvegarde, de la supervision etc…afin de pouvoir évaluer les charges pour chacune.

Lors de revues régulières avec la maitrise d'œuvre et l'exploitation, nous avons défini le workflow à respecter comme :

- la date de livraison des Produits Logiciels Intégrés,
- le dossier d'exploitation à fournir par la MOE,
- les différentes normes à prendre en compte lors de la future Mise en Production (Exemple : SOX),
- date effective du prochain Jalon (J1A).

3.8.4 Du J1A vers le J1B

Dans le cadre de ce projet, le Jalon J1A a été fixé à la date du 26 Juin 2007.

A cette date, la machine de pré-production, nommée IBSAMS02, a été installée et préparée par la Direction Technique.

Les livrables applicatifs doivent être mis à disposition par la maitrise d'œuvre afin d'être testé sur le nouveau serveur.

Les premiers tests de sauvegardes/restauration du système sont effectués et validés.

Des points d'informations, avec la maitrise d'œuvre et les équipes d'exploitation et d'intégration, avaient pour but de prévenir les éventuels imprévus, ou retard, que pourraient générer ces divers tests.

Mon rôle de chef de projet MEP est également de vérifier que tout les pré-requis (exemple : installation de la supervision, tests d'exploitabilités…) sont validés, afin de pouvoir confirmer la date du J1B.
Dans notre cas, la date du J1B a été fixée au 3 octobre 2007.

3.8.5 Du J1B vers le J2

Dans mon projet, le J1B va consister à basculer les flux de production vers le serveur de pré-production IBSAMS02.

Pour ce type d'opération, en collaboration avec les diverses équipes techniques, nous avons établit un macro-planning des tâches à effectuer le jour de la bascule.
Mon rôle a été de le faire respecter et de coordonner les actions des différents acteurs concernés.

Après une période d'observation d'une semaine, période défini en accord avec la maitrise d'œuvre, le serveur de production PNSAMS02 pourra être arrêté. Au bout de 7 jours, il sera mis à disposition de la direction technique afin d'être migrer vers windows2003.
Ce délai est une sécurité afin de pouvoir effectuer un retour-arrière sur l'opération en cas de problème majeur.

Durant cette période de sécurité, le chef de projet MEP initialise et rédige un PV de recette d'exploitabilité provisoire. On s'appuiera, avec l'équipe d'intégration et la maitrise d'œuvre, sur ce document pour définir les derniers détails à résoudre avant le J2.

3.8.6 Le J2

L'opération consistera à remettre le serveur PNSAMS02 en production et à basculer le second serveur en mode « backup ».

Je dois vérifier, que la maitrise d'œuvre aura fourni les documentations nécessaires à l'exploitation (cahier d'exploitation, cahier de reprise applicatif, cahier de supervision), avant validation.

Mon rôle consiste à prendre en charge la communication du projet. Cela se traduit, par exemple, par monter une réunion d'information sur les nouveautés du projet afin de les présenter aux exploitants.

Je devrais m'assurer également de la bonne tenue du macro-planning de bascule, testé lors du J1B.

Le J2 du projet est prévu pour le 03 novembre 2007.

3.8.7 Le J2A

Le J2A est l'aboutissement du projet, le chef de projet mise en production doit :

- s'assurer que toutes les documentations ont été délivrées et sont disponibles pour les exploitants,
- rédiger le PV de recette d'exploitabilité définitive,
- vérifier et produire les documentations nécessaires afin de prouver la conformité aux normes de sécurité (SOX, respect des règles de sécurité lors de la MEP…).

3.9 Apport personnel par rapports à la formation

Être chef de projet mise en production, c'est être le point d'entrée de l'exploitation.
Le CPMEP a un rôle de coordinateur entre la maitrise d'œuvre et l'exploitation.

Il organise des revues régulières avec la MOE et l'équipe d'intégration de production, afin de s'assurer que le planning, les normes, etc… seront bien respectées.

Le fait d'avoir étudié durant mon cursus théorique :

- les relations Maîtrise d'Ouvrage, Maîtrise D'Œuvre et Production dans un S.I.
- les normes, (ITIL, etc…),
- intégration d'une application en production,
- conseil d'intégration dans le SI,
- Windows 2003server,

m'ont permit d'avoir les connaissances nécessaires, tant relationnelles que techniques, afin de mener à bien mon rôle de chef de projet mise en production et d'amener prochainement ce projet à son terme.

4 Conclusion

L'accompagnement sur un projet de système d'information, tel que la refonte des processus de mise en production, apparaît comme un enjeu majeur nécessitant un travail de préparation par le biais d'un diagnostic, d'une analyse d'impacts, qui conditionnent les décisions à suivre.
L'ensemble des problématiques sont délicates à maîtriser, ainsi que la mise en œuvre de leurs solutions potentielles.

Le chef de projet mise en production est un coordinateur.
La base de son travail consiste à coordonner toutes les équipes devant intervenir sur le projet, jusqu'à la mise en production.
La finalité étant d'intégrer parfaitement la nouvelle application dans le Système d'Information, tout en prenant en compte les contraintes de l'exploitation.

Une grande attention doit être portée à la préparation de la réunion de lancement. La communication à destination des différents partenaires est l'occasion d'expliquer l'objectif du projet et l'intérêt pour l'organisation.
Il permet de présenter les outils de communication qui seront utilisés tout au long du projet, réunion de suivi de projet, plan de travail en commun, diagramme des tâches et les jalons importants. Il est judicieux de profiter de ce moment pour tenter de mettre en confiance les différents intervenants.
Le chef de projet MEP doit avoir en permanence une idée précise des différents objectifs opérationnels. Pour tout projet le couple paramètres délais/coût doit être maîtrisé avec précision.

Ces projets révèlent l'intérêt et l'enrichissement, leur complémentarité est intéressante, car elle permet de mettre en place une méthode théorique et ensuite de la mettre en pratique en environnement de production.

5 Glossaire

Accronymes	Définitions
DT	Direction Technique
DPSIF	Direction de la Production SI Facturation
DDSI	Direction Developpement du Système d'Information
DOSI	Direction des Opérations du SI
CPMEP	Chef de Projet Mise En Production
MEP	Mise En Production
DRP	Disaster Recovery Plan
CEE	Cahier des Exigences d'Exploitabilité
CEP	Cahier des Exigences Produits
SLA	Service Level Agreement
GASSI	Gestionnaire d'Accès Sécurisé interne au Système d'Information
SISAME	Sécurisation de l'Accès aux Machines pour les Exploitants
TDIMG	Télé Diagnostique et télé Intervention en Mode Graphique

6 Annexes

6.1 SLA

CONVENTION DE SERVICE
EXPLOITATION D'APPLICATIONS

Nom_de_l'application_+code BASICAT
GxRy
Nom_de_la_Division

SERVICE LEVEL AGREEMENT
CONVENTION N° *XXXXXXXXXX*

(les données en police rouge sont à compléter avec l'accord du Client et du Prestataire)

La présente Convention est conclue entre :

d'une part,

Monsieur le Directeur Exécutif de la Division *Nom_de _la_Dvision* représenté par :
Monsieur, Madame le Directeur de *xxx*
Ci-après désigné "**le Client**"

et d'autre part,

Monsieur le Directeur de la Direction des Opérations du SI représenté par :
Monsieur, Madame le Directeur de la Direction Clients et Projets *xxx*
Ci-après désigné "**le Prestataire**"

Ce dernier est chargé de mener à bien les actions et de respecter les engagements décrits ci-après, afin de faire aboutir les opérations dans les conditions de délais, de résultats et de coûts convenus.

Prestataire	**Client**
Le Directeur Clients et Projets *xxx* DOSI	*Fonction*
Le JJ/MM/AAAA	*Le JJ/MM/AAAA*
Prénom NOM	*Prénom NOM*
Signature	*Signature*

Références documentaires

Références documentaires	Version	Référence/Localisation
Catalogue des services de la DOSI : - Service d'Exploitation d'Applications	V1.2	Site intranet de la DOSI, rubrique « Offres de services »
Conditions Générales de la Convention de Service d'Exploitation d'Applications	V1.3	Site intranet de la DOSI, rubrique « Offres de services »
Accord Budgétaire	V1.1	*A compléter*
Dossier d'exploitation : - le cahier d'installation, le cahier d'exploitation, le cahier des flux, le cahier de sécurité, …		*A compléter*
Dossier d'Architecture Technique		*A compléter*
Plan de Reprise Applicatif		*A compléter ou préciser « non existant »*

1. Objet du document

La Convention de Service est constituée des documents : Conditions Générales, Service Level Agreement et Accord Budgétaire.

Le présent SLA précise les engagements de la DOSI pour l'exploitation de l'application *Nom_de_l'application* à partir de la version *GxRy* jusqu'à dénonciation de ce SLA par l'une des deux parties.

2. Présentation de l'application

Décrire ici par exemple :

Objet de l'application	Gestion centralisée des prestations internes
Périmètre concerné par le SLA	*Tout par défaut, sinon préciser si serveur de données, d'application ou Web*
Plage d'ouverture du transactionnel	*Plage d'ouverture vue des utilisateurs*
Plage d'ouverture du service	*Plage d'ouverture du service*
Utilisateurs	*Nombre potentiel, simultané, interne , externe FT*
Interfaces	*Fréquence, positionnement amont/aval, retard admissible, nombre d'interfaces potentiels*

3. Reprise de l'Applicatif sur Sinistre

Choisir et cocher (☒) le(s) cas applicable(s)s et supprimer le(s) autre(s) cas

Si besoin préciser ou détailler le périmètre concerné (serveurs de données, d'application ou Web)

❒ Un Plan de Reprise Applicatif (PRA) existe et ce plan s'appuie :

- ❒ sur une architecture répartie entre plusieurs sites (au moins deux) et les procédures d'exploitation associées, le tout permettant d'assurer une continuité du fonctionnement de l'application en cas de sinistre d'un des sites.
- ❒ une ou plusieurs plate-formes de secours identifiées avec leurs procédures associées pour une reprise de l'application sur un site distant en cas de sinistre de l'application sur le site de production.

- *indiquer les références du PRA dans les références documentaires du SLA*
- *indiquer les engagements DRAS et/ou RTO, RPO et Fréquence de test, dans le paragraphe suivant (prestations)*

❒ Une externalisation des données de l'application est en place (sans plate-forme de secours distante)

- *indiquer l' engagement RPO, voire la fréquence de test dans le paragraphe suivant (prestations)*

Il n'y a pas de PRA.De fait le prestataire n'est nullement engagé sur une reprise des données et de l'application en cas de sinistre applicatif ou site informatique. (Cependant préciser les moyens éventuels mis en place)

4. Prestations réalisées et engagements du prestataire

4.1 Prestations et Niveaux de prestation

Prestations standards	Niveaux de prestation	Contenu de la prestation standard
Exploitation TP	*Se référer au catalogue*	*Contenu de la prestation standard* - *heures d'ouverture* - *heures d'intervention*
Exploitation Batch	*Se référer au catalogue*	*Contenu de la prestation standard*
Sauvegardes & Restaurations	*Se référer au catalogue*	Préciser obligatoirement les paramètres suivant : - *nature : système, application, données applicatives, logs de connexion pour les applications hors GASSI* - *mode : totale, incrémentale,* - *fréquence : quotidienne, hebdomadaire,suivant exigences du client* - *durée de rétention des sauvegardes* - *externalisation des données*
Supervision	*Se référer au catalogue*	*Contenu de la prestation standard*
Prestations optionnelles	**Niveaux de prestation**	**Contenu de la prestation optionnelle**
Soutien applicatif nuit et week end	*Se référer au catalogue*	*Compléments par rapport au contenu de la prestation optionnelle*
Reprise Applicative (sur sinistre)	*Se référer au catalogue*	*Le Recovery Time Objective (délai de reprise sur sinistre) est mesuré et validé en MEP si des moyens ont été prévus..Il devient contractuel si un test de reprise est contractualisé. Compléments par rapport au contenu de la prestation optionnelle*
Travaux batch supplémentaires	*Se référer au catalogue*	*Compléments par rapport au contenu de la prestation optionnelle*
Supervision non standard	*Se référer au catalogue*	*Compléments par rapport au contenu de la prestation optionnelle*
Tableau de bord SLA	*Se référer au catalogue*	*Compléments par rapport au contenu de la prestation optionnelle*
Prestations spécifiques		**Contenu de la prestation spécifique**
A décrire		*A décrire*

4.2 Engagements QS

Prestations standards	Indicateurs		Engagement QS	Type d'engagement
	Description	**Nom**		
Exploitation TP	Taux de disponibilité (vu de la DOSI)	DISPO_SU	*Seuil = xx %*	Contractuel
	Taux de disponibilité (vu de l'utilisateur)	DISPO_U		Informatif
	Nombre total d'incidents > 5mn	NB_TT	*Seuil = n*	*Informatif/Contractuel*
	Durée de l'incident le plus long	TT_MAX_D	*Seuil = jj,hh*	*Informatif/Contractuel*
Exploitation Batch	*Indicateur et fiche label à créer*	*RPB*		*Informatif/Contractuel*
Sauvegardes & Restaurations	Délai de reprise suite à un incident *(hors domaines de responsabilité réseau et maintenance applicative)*	D_RI	Seuil = RTO benign = *jj,hh*	*Informatif/Contractuel*
	Perte maximale de données sur incident		Seuil = RPO benign = *hh*	
	Test de restauration des sauvegardes	*T_RD*	*Fréquence Test = n/an*	*Contractuel*
	Rétention des sauvegardes		*Durée de la rétention = jj*	*Contractuel*
Prestations optionnelles	**Indicateurs**		**Engagement QS**	**Type d'engagement**
	Drescription	**Nom**		
Reprise Applicative (sur sinistre)	*Perte de donnée maximale admise*		*Seuil = RPO =jj,hh*	*Informatif/Contractuel*
	Délai de restauration de l'application sur sinistre		*Seuil DRAS = jj,hh*	*Informatif/Contractuel*
	Durée maximale d'indisponibilité totale de l'application		*Seuil = RTO= jj,hh*	*Informatif/Contractuel*
	Nombre de tests de Reprise d'Applicatif à faire par an	*T_RA*	*Fréquence Test = n / an*	*Contractuel*
Prestations spécifiques	**Indicateurs**		**Engagement QS**	**Type d'engagement**
	Description	**Nom**		

5.Suivi des prestations réalisées

Se référer aux types de réunions décrites dans les Conditions Générales de la Convention de Service.

Type	Fréquence	Organisateur	Participants	Ordre du jour
R1	*A compléter*	*A compléter*	*A compléter*	*A compléter*
R2	*A compléter*	*A compléter*	*A compléter*	*A compléter*
R3	*A compléter*	*A compléter*	*A compléter*	*A compléter*

6. Conditions d'arrêt de l'application

En plus des cas d'arrêt de la Convention de Service prévus dans les Conditions Générales, la présente Convention de Service est conclue pour une durée d'1 an avec tacite reconduction.

Quelques rappels sur les conditions de durée de la Convention de Service, extrait des Conditions Générales :

- Les engagements de service prennent fin à la date d'arrêt de l'application,
- La demande d'arrêt de l'exploitation de l'application doit parvenir officiellement au moins 2 mois avant la date souhaitée,
- La facturation s'arrête au dernier jour du mois suivant la date d'arrêt effective de l'exploitation,
- Si la demande ne respecte pas le délai de préavis, la facturation s'arrête au dernier jour du troisième mois suivant cette date d'arrêt effective.

7- Accord Budgétaire

L'accord budgétaire de la Convention de Service est décrit dans un document séparé. Il est fourni une première fois à l'initialisation de la Convention de Service et est susceptible d'être révisé semestriellement ou annuellement.

Annexe 1 : les interlocuteurs

Les interlocuteurs identifiés pour la Convention de Service sont cités dans les tableaux ci-dessous.

Interlocuteurs du Prestataire

Prénom NOM	Entité	Fonction	Coordonnées téléphoniques et Email

Interlocuteurs du Client

Prénom NOM	Entité	Fonction	Coordonnées téléphoniques et Email

Annexe 2 : Fiche label Indicateur spécifique XXXX

FICHE LABEL INDICATEUR DOSI

NOM :		LIBELLE :	

SUIVI EN TABLEAU DE BORD DOSI ? : Oui / Non	

OBJECTIF DE L'INDICATEUR :

DESCRIPTION / DEFINITION :

PERIODICITE :		UNITE :	

PERIMETRE :

FORMULE DE CALCUL :

REFERENCES / OBJECTIFS 2005 :

Responsable :		Correspondant :	

Date de production :		Circuit de validation :	
		Calcul et Analyse : Validation :	

6.2 Cahier des Exigences d'Exploitabilité

Exigences d'exploitabilité ***Ce formulaire est à remettre au CP MOE. Il doit être intégré dans le Cahier des Exigences Produit.***	***Référence :*** ***DSI/REF/FEXE001D*** ***Version du document :*** ***SnFn*** ***Date Mise à jour :*** ***jj/mm/aaaa***
Projet :	***Version du projet :*** ***GxRy***

Rédaction		***Vérification***		***Approbation***	
Nom		Nom		Nom	
Date		Date		Date	

Dans ce qui suit, toutes les annotations en vert constituent des aides et sont destinées à être enlevées par vos soins de votre document final

L'objectif de ce document est de proposer un formulaire permettant de consigner les exigences d'exploitabilité exprimées par DOSI pour le projet.

L'alimentation du formulaire sera faite en collaboration avec la MOE du projet, au cours de la phase de mûrissement du projet (J-1→J0).

CONTEXTE

Présentation

Présentation succincte de l'application et du projet
(s'appuyer sur demande de contribution et sur FT CARTO)

Caractéristiques de l'application

Différentiation

OS

FT CARTO

N° FT CARTO :

Code BASICAT :

Plate-forme virtualisée : Oui Non
Plate-forme mutualisée : Oui Non
Prototype : : Oui Non

Caractéristiques du projet

DAT

Date	Version document	Version applicative
xx/xx/xx	S0F0	G1R0
xx/xx/xx	S1F0	G2R0

Modification liée à cette version :

CVAT

Avis du CVAT :

Date	Version document	Version applicative
xx/xx/xx	S0F0	G1R0
xx/xx/xx	S1F0	G2R0

Avis donné à l'occasion de cette version :

Plan de nommage

Il doit faire partie du DAT

Existence :

Date	Version document	Version applicative
xx/xx/xx	S0F0	G1R0
xx/xx/xx	S1F0	G2R0

Plan de nommage défini pour cette version :

Le plan de nommage est obligatoire

- ☒ *pour une nouvelle application*
- ☒ *pour une nouvelle architecture*
- ☒ *pour une évolution de l'architecture*

EXIGENGES D'EXPLOITABILITE STANDARD

Ces exigences concernent essentiellement les OS UNIX, LINUX et WINDOWS

Normes, règles et notes d'ingénierie, notes techniques applicables au projet :

Pour les OS UNIX et WINDOWS, la **MOE** s'appuiera sur le Cahier des Charges Techniques d'Exploitabilité (**CCTE**) en vigueur au J0. Celui-ci présente les normes en vigueur sur les points suivants :

- **DOLLARU**
  Présentation des tâches gérées par $U, de la planification des tâches, de l'arrêt démarrage des serveurs, …

- **PATROL**
  - Présentation des KM obligatoires, de l'organisation de la vue PATROL
  - Prise en compte du mode cluster, de la définition des niveaux d'alarming

- **RHM**

- **NETBACKUP**
  Présentation d'un plan type de sauvegarde

- **GESTION DES FICHIERS LOGS**

- **REBOOT DES SERVEURS**

- **REGLES DE SECURITE**

Livraison et référencement de l'application

Tous les produits logiciels livrés, sans exception aucune, devront l'être dans le **référentiel 26D** en respectant les procédures afférentes.

Livraison	**oui**	**non**
Applicatif		
paramétrage des flux		
Package de PL type		
Scripts dollaru (ordonnancement)		
config Patrol		
BDD		

Intégration serveur, système d'exploitation et logiciel

Les **normes** applicables sont celles référencées dans **@rchimède et PL@TON.**

Recette d'exploitabilité

Il est attendu de la part de l'exploitant une phase de recette d'exploitabilité.
La phase sera décrite en suivi de projet
Elle pourra s'appuyer sur un cahier de tests d'exploitabilité
Elle fera d'objet d'un compte-rendu de recette d'exploitabilité

EXIGENCES LIEES AU PROJET

Organisation de l'exploitabilité au sein du projet

Acteurs

MOA :	
CP MOE :	
Responsable exploitabilité MOE :	
CP MEP :	
Equipe d'exploitabilité :	

Partenaire externe : oui non

Plate-formes

Présentation détaillée dans DAT

NOMBRE DE SERVEURS DE PRODUCTION :

SERVEURS DE PRE-PRODUCTION : ☐ OUI ☐ NON NOMBRE :
SERVEURS DE BACK UP : ☐ OUI ☐ NON NOMBRE :
BACK UP MUTUALISE AVEC PRO-PROD : ☐ OUI ☐ NON

Si le serveur de pré-production sert pour la phase d'intégration, la MOE se concertera avec DOSI pour définir un planning de recette pour que les deux recettes (intégration et exploitabilité) ne se télescopent pas. La recette d'exploitabilité sera prioritaire à la recette d'intégration.

Pré-requis : plate-formes remises à niveau si plate-forme utilisée en intégration.

Exigences spécifiques au projet

À définir.

Reprise du plan d'action élaboré lors de la dernière version

Livrables

Livrables attendus de la MOE

	Période livraison prévue	Obligatoire Facultatif	Commentaires
Dossier d'architecture technique	*avant J0*	O	
Dossier d'architecture fonctionnelle	*avant J0*	F	*nécessaire pour une nouvelle application ou une évolution majeure de l'application*
Avis du CVAT	*avant J0*	F	*si passage en CVAT*
Cahier des flux	*avant J1A*	F	*Obligatoire si application ayant des flux*
Cahier de sécurité (PRA, Partie sauvegardes, habilitations, …)	*avant J1A*	F	*Obligatoire si évolution sur ce thème*
Cahier des charges de supervision Cahier de supervision	*avant J1A*	F	*Obligatoire si évolution sur la supervision*
Cahier des charges de l'ordonnancement cahier d'ordonnancement	*avant J1A*	F	*Obligatoire si évolution sur l'ordonnancement*
Plan de nommage	*avant J1A*	F	*Obligatoire si évolution technique*
Cahier d'installation / Désinstallation	*avant J1A*	O	
Fiches d'exploitation	*1 mois avant J1B*	F	*Obligatoire si évolution de l'exploitation*
Fiches consignes	*1 mois avant J1B*	F	*Obligatoire si évolution de l'exploitation*
Contrat de MPP (ou MPS)	*avant J1B*	O	*DOSI s'engage à travers ce contrat*
MSAP	*avant J2*	F	*Si évolution de la chaine de soutien*

Livrables attendus des installateurs (DOSI)

	Période livraison prévue	Obligatoire Facultatif	Commentaires
Dossier de Configuration Technique	*avant J1A*	F	*Obligatoire si évolution de la plate-forme*
PV de livraison (référentiel 26[E], sauvegardes système opérationnelles, …)	*avant J1A*	F	*Obligatoire si nouveaux serveurs*

Livrables de suivi du projet (CPMEP DOSI)

	Période livraison prévue	Obligatoire Facultatif	Commentaires
PTCE	*après J0*	O	*Adaptation au projet – utilisé tout au long du projet*
Plan d'action élaboré lors de la dernière version	*après J0*	F	
PV de recette J1B	*avant J1B*	F	*Obiligatoire si passage éxémètre prévu*
PV de recette J2	*avant J2*	F	*Obligatoire si passage éxémètre prévu*
PV de recette Post J2	*avant J2A*	F	*Obligatoire si passage éxémètre prévu*

Livrables élaborés par équipe d'exploitabilité (DOSI)

	Période livraison prévue	Obligatoire Facultatif	Commentaires
Dossier des tests d'exploitabilité	*avant J1A*	O	
Déclaration habilitations aux serveurs	*avant J1B*	F	*obligatoire si nouvelles habilitations*
Complétude de la 26E	*avant J2*	F	*obligatoire si nouvelles données*

Livrables élaborés par le Responsable de Compte (DOSI)

SLA	*après J2*	F	*Obligatoire si évolution*

Exigences sécurité

La MOE respectera les **règles de sécurité** du groupe FT.

Exemples :

- *ne pas utiliser FTP ou rcp pour les transferts de fichiers*
- *ne pas utiliser le compte « root » pour des tâches d'exploitation*

L'accès aux serveurs (Exploitants et MOE) devra être défini à travers SISAME (TDIMG) pour UNIX, LINUX

- Faire un audit sécurité à l'aide de l'outil Sécurix – objectif : Conformité RSSI : Oui Non
- Faire un audit de vulnérabilité réseau à l'aide des outils Nessus et Intranode : Oui Non

Si ces audits sont digilentés avant la fin du projet, un plan d'actions de mise en conformité (si nécessaire) sera mis en place. Les points bloquants devront être traités avant la fin du projet.

Exigences Base de Données

À développer

Avoir un capacity planning, une stratégie des purges, stratégie d'archivage

Liste des fiches d'exploitabilité sélectionnées pour le projet

DATE DU DERNIER EXEMETRE :

A L'OCCASION D'UN NOUVEAU PROJET : ☐ OUI ☐ NON (MESURE DE L'APPLICATION)

EXEMETRE PREVU POUR CETTE VERSION : ☐ OUI ☐ NON

Le périmètre des fiches retenues pour l'évaluation de l'exploitabilité est décrit dans le tableau ci-dessous (si passage éxémètre prévu).

La colonne "Std" donnent les options de la norme Agathone, les colonnes "Projet" reprennent les options retenues lors de la précédente version