



Ecole Nationale Supérieure d'Informatique
et d'Analyse des Systèmes

OMNIDATA[®]

Mémoire de Projet de Fin d'Études

Pour l'Obtention du Titre

D'Ingénieur d'État en Informatique

Option

Sécurité des Systèmes d'Information

Sujet

*Refonte de la solution de Reporting réglementaire bancaire pour
les marchés des Changes et Monétaires*

(BRS MCM)

Soutenu par :

Mlle. Ilham BELGHOUL

Jury :

M. Abdelaziz DOUKKALI SDIGUI Président (ENSIAS)

Mme . Hanane EL BAKKALI Encadrante (ENSIAS)

M . Boubker REGRAGUI Rapporteur Président (ENSIAS)

M . Akram ZOUHAIR Encadrant (OMNIDATA)

Dédicace

À mes très chers parents ;

Aucun mot, aucune dédicace ne saurait exprimer mon respect, ma considération et mon amour éternel pour les sacrifices que vous avez consentis pour mon instruction et mon bien être.

À mes très chères sœurs et mon cher frère;

*Nul mot ne pourra exprimer ma gratitude envers vous
À toute personne qui de près ou du loin m'a fait part des renseignements nécessaires à mon stage et mon rapport ;*

À mon cher ami Najib El Houari ;

À mes chers amis ;

Pour tous les instants inoubliables que j'ai passés avec vous, je vous remercie beaucoup ;

Je vous dédie spécialement mon travail de fin d'étude et c'est grâce à vous que je suis ce que je suis aujourd'hui ;

À mon âme sœur

À la fin d'une étape inoubliable;

Et au début d'une autre ;

Je vous aime tous ;

Ilham

Remerciements

Je remercie l'école nationale supérieure d'informatique et d'analyse des systèmes (ENSIAS) pour la formation qu'elle m'a dispensée et qui m'a permis d'acquérir une expérience valorisante dans le monde du travail.

Je tiens à remercier, tout spécialement, Monsieur **Yassine CHAHBI**, directeur de la division Business Intelligence à OMNIDATA, de m'avoir accueilli pour que je puisse effectuer, dans de bonnes conditions, mon projet de fin d'études. Je lui suis très reconnaissante de la confiance qu'il m'a témoignée et je le remercie encore d'avoir mis à ma disposition les moyens nécessaires en vue de la réalisation de mon projet de fin d'études.

Je tiens à témoigner, tout particulièrement, ma reconnaissance à Monsieur **Akram ZOUHAIR**, mon encadrant de stage, qui a su m'épauler, m'orienter, me conseiller et répondre à toutes les questions que je lui posais. Qu'il en soit, ici, très vivement, remercié. Toujours disponible, il m'a permis de partager son expérience professionnelle.

Mes remerciements vont également à Madame **Hanane EL BAKKALI**, mon encadrant de stage, qui a su, à bon escient, me remotiver et tracer les lignes directrices de mon Mémoire.

Je tiens à exprimer mes sincères remerciements à tous les membres d'**OMNIDATA** qui ont fait preuve d'esprit de groupe et de solidarité inlassable durant toute la durée du stage.

Enfin, je tiens à remercier les membres du jury pour leur bienveillance à vouloir évaluer mon travail, ainsi que toute personne ayant participé de près ou de loin au bon déroulement de ce travail.

Résumé

Le présent rapport est une synthèse du travail effectué dans le cadre du projet de fin d'études au sein de la société OMNIDATA. L'objectif du projet est la refonte de la solution de Reporting pour les marché de change et monétaire BRS MCM (Bank Reporting System pour Marché de change et monétaire)

Ma mission dans le cadre de ce projet consistait à étudier la solution existante et de dégager ses limites et ses vulnérabilités afin de pouvoir procéder à sa refonte sous une nouvelle technologie.

En effet, ce projet a pour objectif principal de proposer une nouvelle solution BRS MCM avec une nouvelle interface web ainsi qu'un temps de réponse plus court, tout en intégrant les aspects Sécurité. Pour atteindre cet objectif, une analyse détaillée des impacts fonctionnels et techniques a été effectuée afin de saisir la complexité de l'architecture applicative, pouvoir refaire convenablement la conception et la réalisation de la solution.

Une grande importance a été donnée aux aspects Sécurité de la nouvelle solution. A ce propos, un plan d'action qui commence par une analyse des risques et qui s'inspire des normes ISO 27002/27005 a été établi. La sécurité des flux transmis par les banques et les établissements de crédit à BAM a également été traitée ainsi que la gestion des droits d'accès aux ressources de la solution.

Abstract

This report summarizes the work done in the project graduation within society OMNIDATA. The objective of the project is the redesign of the Reporting solution for the foreign exchange market and monetary BRS MCM (Bank Reporting System for the foreign exchange market and monetary).

Our mission is to study the existing solution and identify its limitations and vulnerabilities, after conducting a detailed analysis of functional and technical impacts to grasp the complexity of the application architecture, then do a risk analysis of the new project and propose an action plan to minimize these risks, re-design and finally manage profiles and users.

We have adopted solutions to control and secure sending statements to the financial statements of banks and credit institutions, to Bank El Maghreb (BAM), we proposed a model to manage users, roles, privileges granted to each role and access profiles of project resources (files and databases).

We also used MEHARI to propose a security policy in its first version by risk analysis and establishing an action plan.

Table des figures

Figure 1 : Les activités d'OMNIDATA	16
Figure 2 : Les chiffres clés d'OMNIDATA entre les années 2007 et 2010	18
Figure 3 : Cycle de vie en cascade	25
Figure 4 : diagramme de GANTT	27
Figure 5 : Architecture générale de BRSMCM.....	31
Figure 6 : Processus de la déclaration sur BRSMCM	33
Figure 7 : Description des différents profils.....	41
Figure 8 : Droits d'accès de l'administrateur aux modules de gestion des	42
Figure 9 : Droits d'accès de l'exploitant aux modules de contrôle et de traitement.....	42
Figure 10 : Droits d'accès de l'administrateur fonctionnel au référentiel de BRS MCM.....	43
Figure 11 : Les rôles et les privilèges pour les utilisateurs.....	43
Figure 12 : Etapes dans la gestion des risques.....	47
Figure 13 : Résumé de l'utilisation MEHARI.....	48
Figure 14 : Echelle de valeurs et classifications.....	49
Figure 15 : Tableau T1 classification des actifs de catégorie « données ».....	53
Figure 16 : Tableau T1 classification des actifs de catégorie « Services »	53
Figure 17 : Tableau T3 classification des actifs « processus de management ».....	54
Figure 18 : Cas d'utilisation du package paramétrage	68
Figure 19 : Cas d'utilisation du package traitement	69
Figure 20 : Cas d'utilisation du package sécurité.....	70
Figure 21 : Cas d'utilisation de gestion du référentiel.....	71
Figure 22 : Diagramme de cas d'utilisation général.....	72
Figure 23 : Diagramme de classes participantes du package sécurité	73
Figure 24 : Diagramme de classes participantes du package paramétrage.....	74
Figure 25 : Cas Diagramme de séquence du package traitement	76
Figure 26 : Historique d'évolution d'APEX.....	81
Figure 27 : Architecture 2-Tiers d'APEX	82
Figure 28 : Utilisation de SSL par le protocole HTTP.....	85
Figure 29 : Ecran d'authentification.....	86
Figure 30 : Menu général de BRS MCM	87
Figure 31 : Ecran chargement des données à partir des fichiers sources.....	87
Figure 32 : Consultation des données « position de change ».....	88
Figure 33 : Contrôle des données à déclarer.....	89
Figure 34 : Document rapport de contrôle des fichiers d'échange	89
Figure 35 : Ecran de génération des fichiers XML	90
Figure 36 : Gestion des profils	90
Figure 37 : Gestion des utilisateurs	90

Liste des tableaux

Tableau 1 : Equipe de la Business Unit BI and CRM	19
Tableau 2 : Les intervenants côté OMNIDATA	23
Tableau 4 : Profils et rôles.....	23
Tableau 5 : Activités majeurs du projet et leurs résultats attendus.....	49
Tableau 6 : Identification des dysfonctionnements redoutés.....	50
Tableau 7 : Actifs de type données et informations	53

Table des matières

Table des figures	7
Liste des tableaux.....	8
Table de matières	9
Glossaire	12
Introduction générale	13
Chapitre 1	
1. Contexte général du projet	16
1.1. Présentation de l'organisme	16
1.1.1. OMNIDATA.....	16
1.1.2. Historique	17
1.1.3. Chiffres clés	18
1.1.4. La Business Unit BI et CRM.....	18
1.2. Contexte du projet	20
1.2.1. Description général du projet	20
1.2.2. Cadrage du projet	22
1.2.3. Planification du projet	26
Conclusion.....	28
2 Chapitre	
Analyse fonctionnelle et organisationnelle	30
2.1. Etude de l'existant	30
2.1.1. Description de la solution BRS-MCM	30
2.1.2. Analyse de l'existant	33
2.2. Expression du cahier des charges	35
2.2.1. Spécifications fonctionnelles	35
2.2.2. Les règles de gestion	36

2.2.3. Spécifications d'organisation et d'exploitation	40
Conclusion	44
Chapitre 3	
3. Analyse des risques et conception.....	46
3.1. Analyse des risques.....	46
3.1.1. Introduction MEHARI	46
3.1.2. Analyse des enjeux et classification	48
3.1.3. Elaboration du plan d'actions	54
3.2. Conception	66
3.2.1. Présentation du langage UML	66
3.2.2. Identification des cas d'utilisation	67
3.2.3. Diagramme de classe	73
3.2.4 Diagramme de séquence	74
Conclusion.....	78
Chapitre 4	
4. Mise en œuvre	79
4.1. Outils utilisés	79
4.1.1. SGBD Oracle 11 g	79
4.1.2. TOAD pour Oracle	80
4.1.3. Oracle Application Express	81
4.1.4. Javascript	81
4.1.5. Langage PL/SQL	84
4.2. Cryptage des données et échanges de clés.....	84
4.2.1. Le package DBMS-CRYPTO	84
4.2.2. Le protocole SSL	84
4.3. Mise en œuvre	85
4.3.1. Les étapes de la mise en œuvre	85
4.3.2. Résultat de la mise en œuvre	86
Conclusion.....	94

Conclusion générale	94
Références bibliographiques	95
Annexes.....	97
Annexe A : Tableau d'impact intrinsèque	98
Annexe B : Tableau des vulnérabilités intrinsèques.....	100
Annexe C : Manuel d'installation d'Oracle APEX.....	102

Glossaire

Acronyme	Définition
APEX	<i>Oracle Application Express</i>
BAM	<i>Bank Al Maghreb</i>
BRS	<i>Bank reporting System</i>
BRS MCM	<i>Bank Reporting System pour Marché de change et monétaire</i>
ISO	<i>Organisation nationale de normalisation</i>
Méhari	<i>Méthode harmonisée d'analyse des risques</i>
SSL	<i>Secure Socket Layer</i>
SWIFT	<i>Société worldwind interbancaire financière de télécommunication</i>
XML	<i>Extensible Markup Language, langage de balisage extensible.</i>

Introduction générale

L'instauration des marchés des changes et monétaires au Maroc en 1996 constitue incontestablement une des principales manifestations concrètes de l'intégration de l'économie marocaine dans le circuit de la mondialisation et de la globalisation financière. Fini le temps où les banques se limitaient à jouer un rôle de « boîte à lettre » entre leurs clients et la Banque Centrale pour acheter ou céder des devises sur la base d'un taux de change administré et indifférencié. Aujourd'hui, les banques marocaines sont dotées de véritables vitrines technologiques, dénommées salles des marchés, habilitées à effectuer des opérations d'achat et de vente de devise dont les taux de change sont librement négociables entre les parties. Grâce à ces nouveaux marchés, les exportateurs et les importateurs marocains peuvent non seulement négocier des taux de change préférentiels, mais aussi se couvrir contre le risque de change.

A ce niveau, le Reporting réglementaire pour les marchés des changes et monétaires constitue la présentation périodique de rapports et bilans analytiques sur les activités et résultats d'une banque ou un établissement de crédit. Afin de répondre à ce besoin de reporting et d'assurer la conformité de transfert des déclarations à Bank Al Maghrib (BAM), la société OMNIDATA a réalisé en 2003 le système BRS MCM (Bank Reporting System pour les marchés des changes et monétaire).

C'est dans ce cadre que s'inscrit mon projet de fin d'études intitulé « Refonte de la solution du Reporting réglementaire bancaire pour les marchés des changes et monétaires ». Il s'agit, en effet, de la refonte de la solution BRS MCM sous une nouvelle technologie.

Ce projet a pour objectif principal de proposer une nouvelle solution BRS MCM avec une nouvelle interface web ainsi qu'un temps de réponse plus court, tout en intégrant les aspects Sécurité. Pour ce faire, un plan d'action qui commence par une analyse des risques et qui s'inspire des normes ISO 27002/27005 a été établi. La sécurité des flux transmis par les banques et les établissements de crédit à BAM a

également été traitée ainsi que la gestion des droits d'accès aux ressources de la solution.

Le présent rapport décrit les principales phases du projet. Il comporte quatre chapitres dont le premier donne une vision générale sur le contexte du projet et l'organisme d'accueil, ainsi que la méthodologie de gestion et de conduite du projet suivie. Le deuxième chapitre présente une étude et analyse de l'existant, une description du cahier des charges, ainsi qu'une analyse fonctionnelle détaillée décrivant les exigences du projet et détaillant les vérifications à effectuer au niveau de chaque état. Ce chapitre permet également de donner les règles de gestion qu'il faut respecter pour la réalisation du projet.

Le troisième chapitre présente une analyse des risques avec la méthode MEHARI en commençant tout d'abord par une analyse des enjeux de la sécurité suivie du plan d'actions qui est le début de l'adaptation d'une politique de sécurité dans sa première version. Ce chapitre traite aussi la conception de la nouvelle solution BRS MCM en réalisant des diagrammes UML. Le dernier chapitre décrit les différentes étapes de la mise en œuvre de la solution retenue et un aperçu sur le travail réalisé.

Contexte général du projet

Ce chapitre présente l'organisme d'accueil, le contexte du projet, ainsi que la méthodologie de gestion et de conduite du projet que j'ai suivie et qui a permis de garantir un bon déroulement dans toutes les phases du projet et un bon respect des délais et de la qualité du travail réalisé. En fin du chapitre je présente le planning qui a été adopté dans le cadre de cette refonte.

1. Contexte général du projet

1.1 . Présentation de l'organisme

1.1.1 . OMNIDATA

OMNIDATA est la première société marocaine de services, de conseil et d'ingénierie dans les technologies de l'information. Leader national dans le domaine des systèmes d'information, OMNIDATA a mobilisé depuis deux décennies les meilleures compétences pour répondre aux impératifs de performance de ses clients en termes de qualité de service, de valeur ajoutée, et de coûts.

OMNIDATA a pour objectif d'aider ses clients à mettre leur Système d'Information au service de leur stratégie à long terme. Pour cela, OMNIDATA offre une large palette de prestations organisées autour des activités suivantes:

- Mise en œuvre et support technique des infrastructures logicielles.
- Formation, assistance et expertise technologique.
- Intégration et implémentation d'applications de gestion pour l'entreprise.
- Conception et développement d'applications spécifiques au Maroc et à l'international.
- Business Intelligence et Customer Relationship Management.

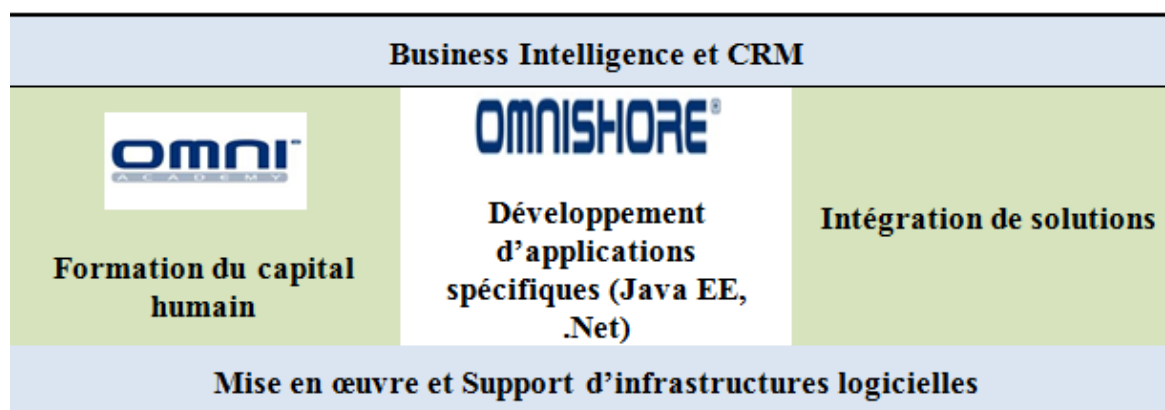


Figure 1 : Les activités d'OMNIDATA

1.1.2. Historique

OMNIDATA est née en 1989. Vingt-quatre ans après sa création, la société est considérée aujourd'hui comme le fleuron du secteur des technologies de l'information au Maroc. OMNIDATA a réussi, au fil de ces années, à consolider son leadership avec une démarche de développement progressive des métiers des technologies de l'information et une recherche permanente de valeur ajoutée. Elle est passée, ainsi, de la distribution et support de produits au développement de systèmes spécifiques puis à l'intégration de progiciels.

L'année 2006 a marqué un tournant dans la vie de l'entreprise à travers l'opération de fusion avec la société de service informatique et d'ingénierie Cap'Info, autre leader des TI au Maroc.

Peu de temps après, OMNIDATA décide d'aller à l'international en créant le département OmniShore qui est maintenant responsable des projets internationaux avec des partenaires (principalement suisses, français et belges), et a un avenir prometteur dans les activités offshore.

OMNIDATA lance en 2008 OmniAcademy. Cette branche est spécialisée dans la formation pour les professionnels dans le domaine des technologies de l'information. OmniAcademy a établi un partenariat avec le leader international dans l'enseignement des nouvelles technologies « OracleUniversity » pour fournir une formation de qualité dans les technologies comme J2EE, le mainframe, l'open source et la sécurité. OmniAcademy est déterminée à améliorer le contexte technologique de professionnels et de maintenir leurs connaissances à jour, non seulement au Maroc, mais dans tous les pays de l'Afrique du Nord.

Afin de prouver que la qualité de ses services est conforme aux normes internationales, l'entreprise a obtenu une accréditation CMMI niveau 2 en 2011.

Premier fournisseur Marocain en systèmes d'information, OMNIDATA est particulièrement active dans le secteur public, le secteur financier et les télécommunications.

1.1.3. Chiffres clés

Les chiffres d'affaires, les ressources et le résultat annuel de la société ont connu une progression remarquable entre les années 2007 et 2010, les diagrammes suivants présentent cette progression ainsi que la répartition des chiffres d'affaires par secteur d'activité et par Business Unit.

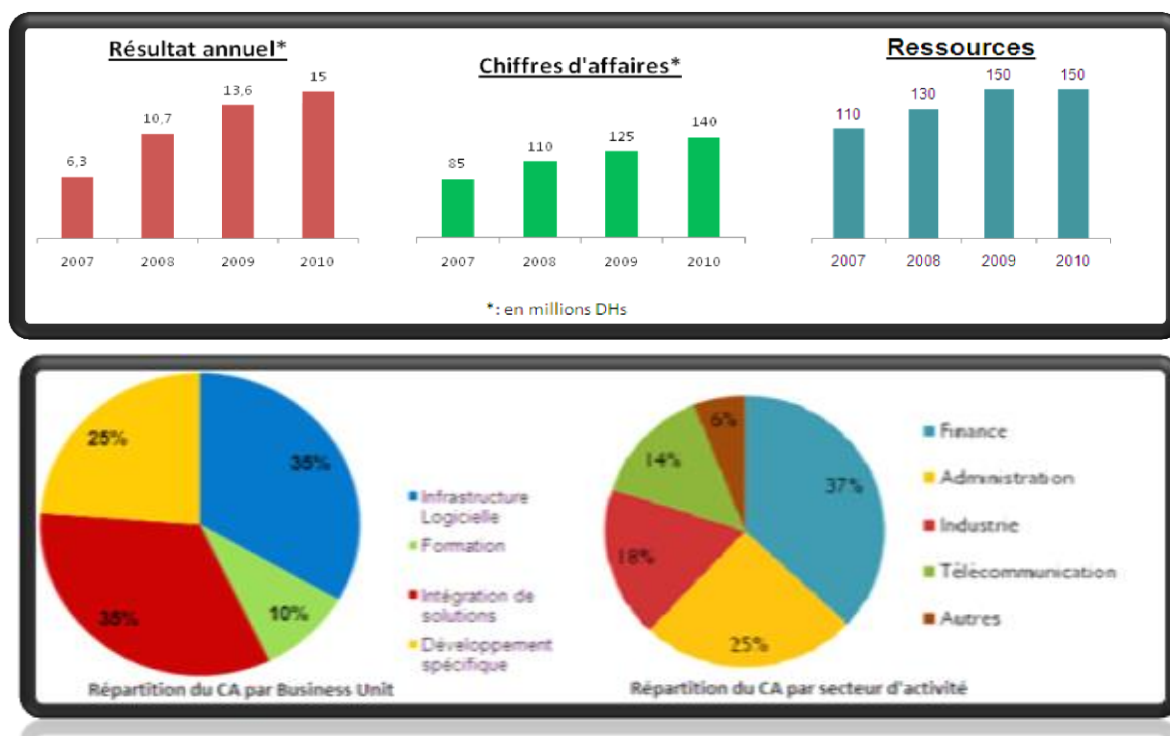


Figure 2 : Les chiffres clés d'OMNIDATA entre les années 2007 et 2010

1.1.4 . La Business Unit BI and CRM

Présentation de l'équipe

L'équipe BI & CRM est une équipe informatique qui a été créée depuis 1999 et est actuellement constituée de 9 Personnes:

Nom & Prénom	Statut
Yassine CHAHBI	Manager BI & CRM
Boutaina LABOUDI	Chef de Projet
Miloud ER RADHA	Consultant
Tarik TADLAOUI	Consultant
Fatima DAOUI	Consultant
Akram Zouhair	Consultant
Smail BARAT	Consultant
Habib ABOUSABER	Consultant
Hicham ELATTARI	Consultant

Tableau 1 : Equipe de la Business Unit BI and CRM

Domaines de Compétences

- Gestion du cycle de vie projet :
 - Recueil des besoins des utilisateurs,
 - Rédaction des spécifications fonctionnelles et techniques,
 - Développement et déploiement des solutions informatiques,
 - Maintenance applicative et corrective,
 - Support et formation utilisateur.

- Expertise technique :
 - Technologies :QlikView, Business Objects, ODI ...
 - Technologie Microsoft : Framework .NET, C#, ASP.NET, VB
 - Progiciels : Oracle E-Business Suite, CRM
 - Informatique décisionnelle.

Des solutions dans différents créneaux ont été mises en place chez des entreprises clientes qui demeurent satisfaites de leurs produits

1.2 . Contexte du projet

1.2.1. Description générale du projet

a- Périmètre du projet

Le projet BRS MCM (Bank Reporting System pour Marché des Changes et Monétaires) s'inscrit dans le cadre du projet BRS. Ce dernier regroupe l'ensemble des applications de Reporting, ces applications sont le cœur des outils opérationnels des clients d'OMNIDATA.[1].

Bank Reporting System (BRS) est un projet de Reporting réglementaire qui permet de générer un certain nombre d'états soit comptables ou non comptables pour être ensuite déclarés à Bank Al Maghrib. BRS comprend 8 projets à savoir :

- COREP
- Marchés des changes et Monétaires
- Etats comptables
- Etats non comptables
- FINREP
- Veille Sectorielle
- Crédit Bureau
- Reporting ALM

Dans le cadre de la réglementation de Bank Al Maghrib (BAM), relative au Reporting des marchés des changes et monétaires pour les Banques et les établissements des crédits, OMNIDATA décide la refonte de la solution BRSMCM (Bank Reporting System pour Marché de Change et Monétaire) qui permet de répondre principalement aux besoins suivants :

- Elaboration des déclarations des marchés avec une fréquence journalière, hebdomadaire ou mensuelle
- Eenrichissement des données manquantes

- Contrôle et l'envoi des déclarations
- Prise en charge des retours BAM.
- Administration des profils/utilisateurs.

C'est dans ce cadre que s'inscrit mon projet de fin d'étude intitulé « Refonte de la solution de Reporting bancaire pour les marchés de change et monétaire (gestion des profils/utilisateurs) »

Problématique et motivation

Vu l'énorme quantité des données gérées par les différents modules de BRS MCM et vu la contrainte de cohérence des données qui doivent respecter un certain nombre de règles il a fallu contrôler les différents flux de données parvenant des différents modules pour assurer un fonctionnement optimal de ces derniers.

Par ailleurs, étant une application critique, qui nécessite un haut niveau de sécurité, la refonte de BRS MCM impose en plus de sa nouvelle conception, une bonne gestion des profils, privilèges et rôles des utilisateurs afin d'assurer une manipulation sécurisée des données et un accès contrôlé aux ressources (Bases de données, fichiers XML, fichiers EXCEL).

c - Contraintes et objectifs

En se basant sur les nouvelles technologies, l'évolution de l'outil BRS MCM devra se faire en respectant des besoins fonctionnels client, mais devra encore répondre aux contraintes suivantes :

- Amélioration de la performance applicative.
- Accessibilité depuis un navigateur web ou via l'intranet (il s'agit donc d'un client léger)
- Accès à l'historique de l'Administrateur ainsi que la gestion des archivages.
- Mise en place d'un mécanisme d'authentification et de recherche centralisé.
- Amélioration de la flexibilité et de la facilité de manipulation par l'utilisateur.
- Administration des profils/utilisateurs.
- Bonne gestion des privilèges et une séparation des rôles bien précise pour les utilisateurs de l'application afin d'éviter des rôles conflictuels.

1.2.2. Cadrage du projet

Cette présente le déroulement de notre projet et ceci en donnant un aperçu sur le planning élaboré au début du stage tout en expliquant le travail effectué durant chaque phase .

a – Déroulement du projet

Avant de commencer notre travail sur le sujet une première réunion avec l'encadrant a été primordiale, où nous avons eu une idée préliminaire concernant le projet. A l'issue de cette dernière, nous avons pu établir un planning prévisionnel pour toute la durée du stage tout en précisant les besoins du projet.

Le projet s'est déroulé selon les phases suivantes :

- ***Détection des vulnérabilités de l'ancienne solution BRS MCM :***
 - Analyse de la solution existante et détection de ces failles de conception et de sécurité.
- ***Analyse des risques de la nouvelle solution :*** utilisation de la méthode de MEHARI pour l'analyse des risques de la solution.
- ***Formation & Développement sous Oracle APEX :*** Formation et documentation sur l'architecture générale de l'outil APEX et les différentes phases de création des travaux, ainsi que l'installation et la configuration de cet outil.
- ***Réalisation sous la plate-forme APEX :***
 - Documentation et spécification des besoins
 - Conception de la solution retenue
 - Réalisation de la solution retenue
- ***Rédaction du rapport et présentation du PFE***

b – Plan assurance qualité

Le plan d'assurance qualité est un livrable qui permet de s'assurer de l'efficacité des activités prévues pour obtenir une qualité requise.

L'objectif du plan d'assurance qualité présenté sur ce rapport consiste à exposer les dispositions mises en œuvre pour satisfaire les exigences du projet qui consiste à la

conception et développement d'une application et à la gestion des profils et des utilisateurs via le contrôle de planning et des tâches qu'assure l'équipe de service couverture sur mesure, la société arrive à livrer un produit de qualité requise.

Les dispositions décrites ci-dessous couvrent le processus de développement du projet en présentant les différents acteurs et leurs tâches à partir de l'analyse des besoins jusqu'à la mise en production du projet.

c – Conduite du projet

Les acteurs qui ont participé à la réalisation du projet et leurs rôles sont résumés comme suit :

Personne	Rôle
M. CHAHBI Yassine	Manager
Mme. LABOUDI Boutaina	Chef de projet
M. ZOUHAIR Akram	Encadrant OMNIDATA
BELGHOUL Ilham	Stagiaire Elève-ingénieure

Tableau 2 : Les intervenants côté OMNIDATA

Chaque rôle se charge d'une action ou ensemble d'actions. Le tableau ci-dessous présente le profil de chaque rôle :

Intervenants	Présentation des besoins	Rédaction	Validation	Suivi	Réalisation
Equipe du projet	X		X	X	
Encadrant OMNIDATA			X	X	
Elève-ingénieure		X			X

Tableau 3 : Profils et rôles

d – Objectifs qualité du projet

En termes de qualité, la solution à réaliser doit atteindre les objectifs suivants :

- **Fiabilité** : le système doit avoir un taux minimal de défaillance, en exécutant avec précision les instructions demandées par l'utilisateur avec gestion de toutes les exceptions ;
- **Disponibilité** : le système doit être accessible au client de la manière la plus simple, la plus ergonomique et ce d'une manière permanente ;
- **Evolutivité** : au fil du temps, le système doit être améliorable ;
- **Réutilisabilité** : lors du développement du projet, on conçoit et met en œuvre des outils exploités dans ce projet. Il doit y avoir la possibilité de ré-exploiter ces outils dans d'autres projets ;
- **Indépendance des outils techniques** : cela s'explique par la possibilité de changer les outils utilisés par d'autres outils meilleurs.
- Lors de l'élaboration du projet, je suis tenue à viser les objectifs qualité et respecter toute règle et norme en vigueur au sein de la société. Je suis aussi chargée de vérifier l'adéquation des fonctionnalités mises en œuvre avec les besoins métiers précisés par l'équipe de pilotage. Mon activité dans le cadre d'assurance et de contrôle est constamment vérifiée par mon encadrant.

e - Modèle du cycle de vie en cascade

Le modèle de cycle de vie en cascade a été mis au point dès 1966, puis formalisé aux alentours de 1970.

Dans ce modèle le principe est simple : chaque phase se termine à une date précise par la production de certains documents ou logiciels. Les résultats sont définis sur la base des interactions entre étapes, ils sont soumis à une revue approfondie et on ne passe à la phase suivante que s'ils sont jugés satisfaisants.

Le modèle original ne comportait pas de possibilité de retour en arrière. Celle-ci a été rajoutée ultérieurement sur la base qu'une étape ne remet en cause que l'étape précédente.[2].

En ce qui concerne mon projet j'ai choisi de travailler avec un modèle en cascade vu qu'il propose au fur et à mesure une démarche de réduction des risques, en minimisant au fur et à mesure l'impact des incertitudes. L'impact d'une incertitude dans la phase de développement étant plus faible que l'impact d'une incertitude dans les phases de Conception ou de Spécifications, plus le projet avance, plus les risques diminuent.

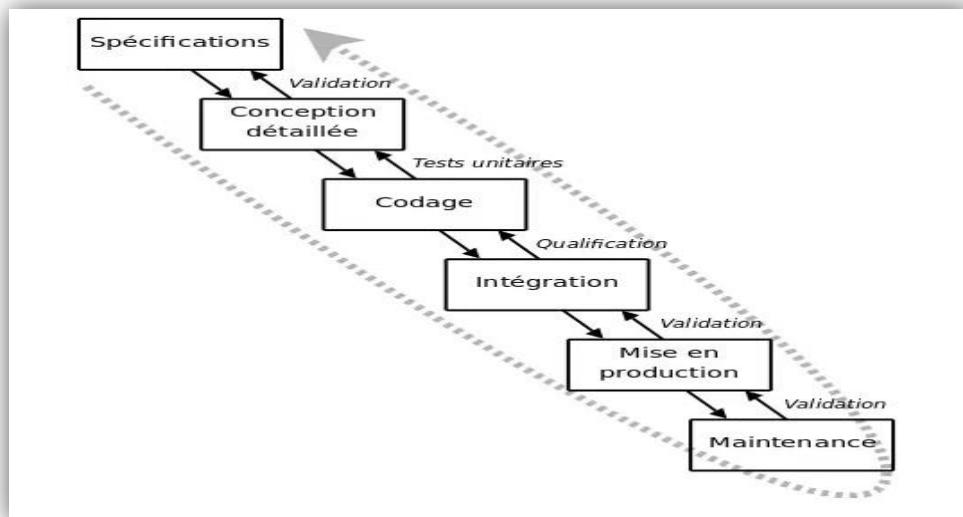


Figure 3 : Cycle de vie en cascade

1.2.3. Planification du projet

Avant de se pencher sur l'étude détaillée du projet, une phase de planification est primordiale afin d'assurer la bonne conduite du projet puisqu'elle participe d'emblée au succès de la démarche.

De ce fait, la nécessité de maîtriser le projet implique la mise en place d'une organisation adaptée en ce qui concerne l'ordonnancement des tâches. En effet, la planification et l'ordonnancement sont des phases essentielles du projet. Il s'agit d'identifier dans un horizon de temps, le meilleur découplage et enchaînement des tâches indispensables à la réalisation du projet.

Pour cet effet, je me suis penchée dès le début du stage à élaborer un planning de tâches pour la réalisation de mon projet. Ce planning s'étale sur 7 différentes phases nécessaires pour le bon déroulement du projet.

A savoir, la phase :

- 1- Prise de connaissance du périmètre OMNIDATA*
- 2- Analyse projet BRS MCM– Existant,*
- 3- Analyse des risques de la nouvelle solution BRS MCM*
- 4- Expression des besoins et contraintes,*
- 5- Formation et Manipulation,*
- 6- Conception (ingénierie des rôles),*
- 7- Développement*
- 8- Test et déploiement.*

Diagramme de Gantt :

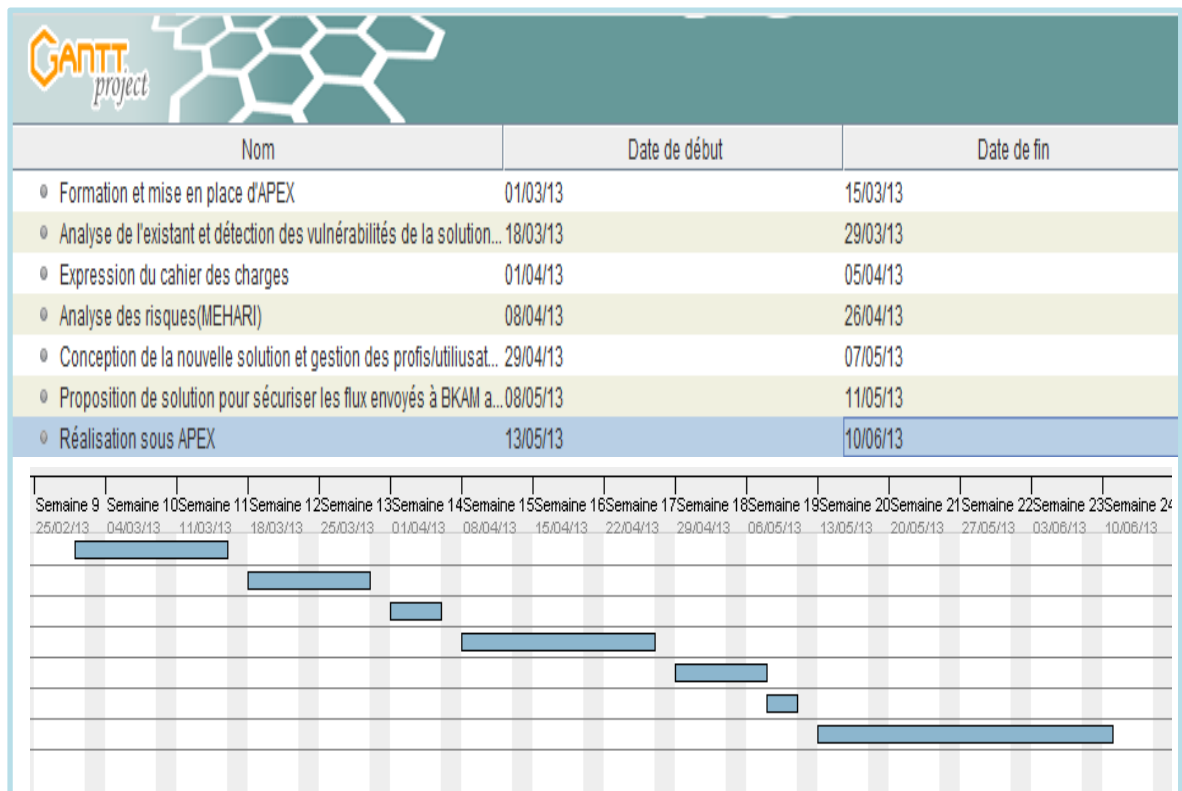


Figure 4 : diagramme de GANTT

Conclusion

Ce chapitre a présenté, d'une part, l'organisme d'accueil, ses missions et son organisation et d'autre part, une vue globale sur le déroulement des différentes phases de gestion de ce projet qui consiste à mettre en place une nouvelle solution de Reporting bancaire pour les marchés des changes et monétaires, de faire une analyse des risques du nouveau projet ainsi que la gestion des profils et des utilisateurs.

Dans le prochain chapitre, il sera question de détailler la phase d'analyse de l'existant, les vulnérabilités de la solution actuelle, le cahier des charges et l'analyse fonctionnelle et organisationnelle détaillée du projet.

Analyse fonctionnelle et organisationnelle

L'analyse est un procédé préliminaire à chaque projet qui a pour objectif de formaliser les premières étapes de développement d'un système pour rendre ce développement plus fidèle aux besoins du client. Ce chapitre présente une étude et analyse de l'existant, une description du cahier des charges, ainsi qu'une analyse fonctionnelle détaillée et une analyse organisationnelle de la solution.

2. Analyse fonctionnelle et organisationnelle

2.1 . Etude de l'existant

L'analyse de l'existant est la première démarche pour identifier les exigences auxquelles le projet doit répondre. Il est important de décrire le contexte du projet permettant d'identifier les interactions mais aussi de mettre le doigt sur les faiblesses et les points de force de la solution BRS MCM.

2.1.1 Description de la solution BRS-MCM

Dans le cadre de la réglementation de Bank Al Maghrib (BAM), relative au Reporting des marchés des changes et monétaires pour les Banques et les établissements de crédit, OMNIDATA a réalisé la solution BRSMCM (Bank Reporting System pour Marché de Change et Monétaire) qui permet de répondre principalement aux besoins suivants :

- L'élaboration des déclarations des marchés avec une fréquence journalière, hebdomadaire ou mensuelle,
- L'enrichissement des données manquantes,
- Le contrôle et l'envoi des déclarations,
- La prise en charge des retours BAM.

L'architecture générale de la solution BRS MCM est composée de trois parties comme le montre la figure suivante :

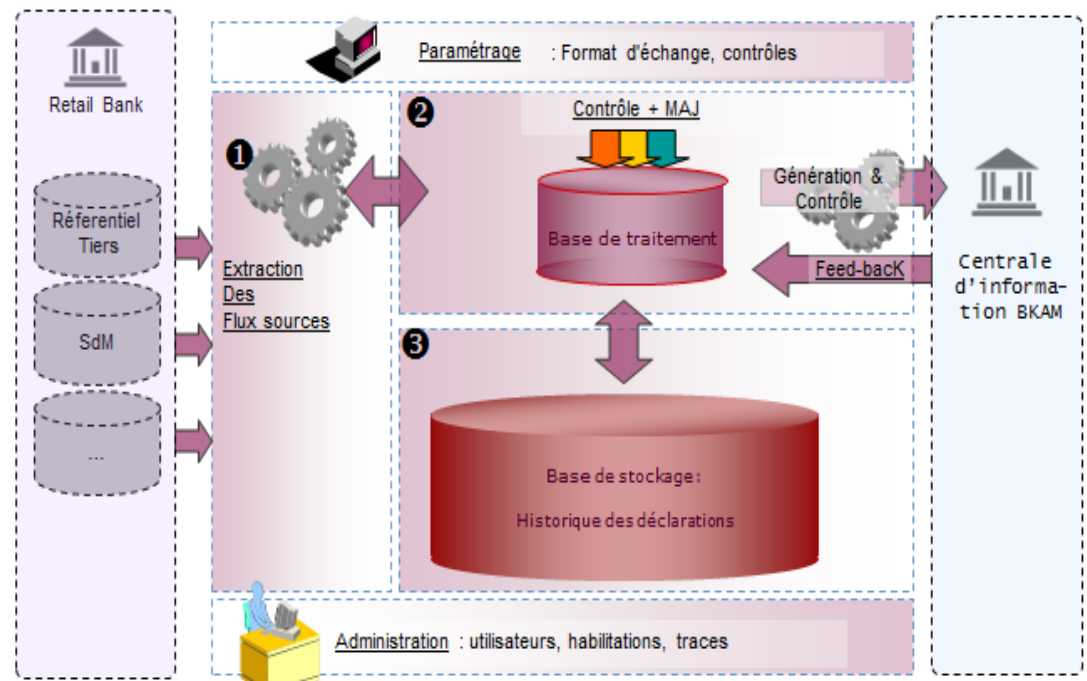


Figure 5 : Architecture générale de BRSMCM

1) Intégration transparentes avec les SI sources :

- Contrôle de la qualité des données chargées
- Transformation des données/enrichissement
- Intégration dans la base de travail

2) Base du travail :

- Validation des données
- Saisi des données complémentaires (cours, notation, données des tiers)
- Simulation et gestion des retours
- Génération des flux XML

3) Traitement des retours :

- Autonomie de l'utilisateur final sur le traitement des lignes rejetées au niveau de la déclaration.

Le processus de génération d'un flux en format XML demandé par BAM suit les étapes suivantes :

- **Préparation du fichier :**

Ouvrir le fichier texte qui se trouve dans un répertoire de travail dans le serveur de l'organisme utilisateur de l'application BRSMCM.

- **Connexion à l'application BRSMCM :**

Entrer le nom de l'utilisateur et son mot de passe.

- **Chargement des flux :**

Charger, par domaine, les flux sources conformément à l'entrée standard de BRSMCM dans l'entrepôt dédié au marché des changes et monétaire.

- **Contrôle du fichier partagé :**

Grâce aux contrôles effectués par BRSMCM, l'utilisateur peut simuler le retour BAM grâce aux logs, les erreurs sont ainsi corrigées en amont.

- **Génération du fichier en format XML :**

Une fois les contrôles sont appliqués et les anomalies relatives aux données sont rectifiées, l'utilisateur peut procéder à la génération, par domaine, des fichiers XML à destination de BAM

- **Lecture du fichier de retour BAM :**

Une fois le fichier retour est disponible dans le répertoire des XML, on peut les lire.

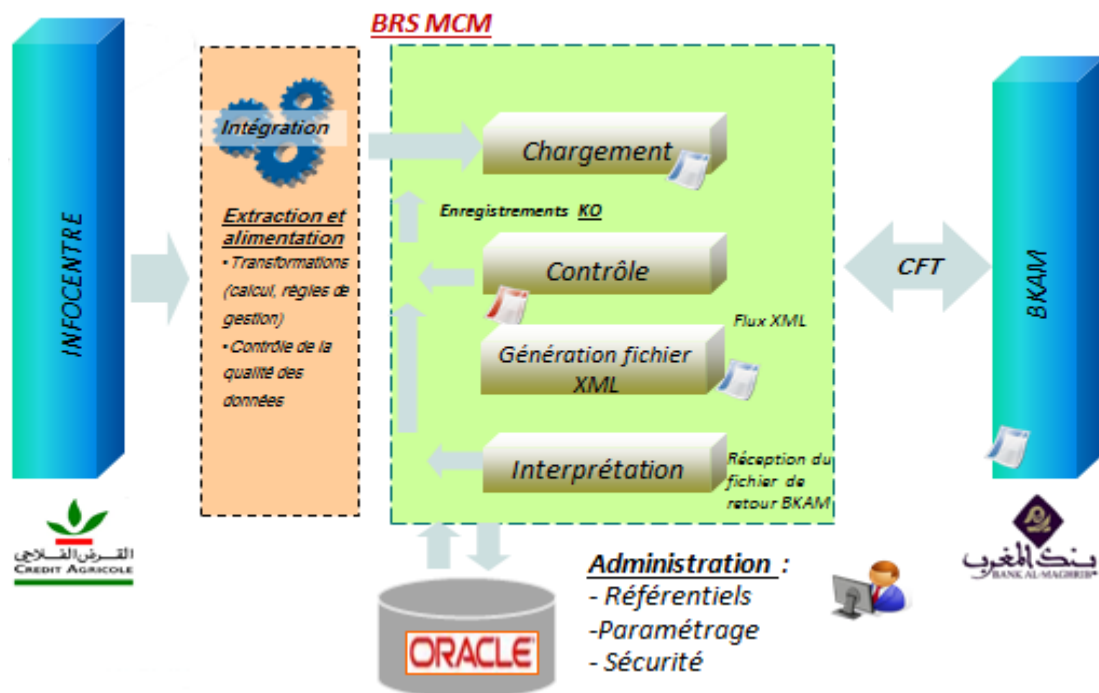


Figure 6 : Processus de la déclaration sur BRSMCM

2.1.2. Analyse de l'existant

La solution de Reporting bancaire pour le marché des changes et monétaire existante possède plusieurs avantages :

- Simplicité, facilité à l'utilisation.
- Stabilité et haute disponibilité.
- Haut niveau d'automatisation.
- Grande satisfaction des clients.

Cependant vu l'âge de la plateforme plusieurs problèmes sont apparus :

- Difficulté de maintenance
- Conséquent BRSMCM sous Oracle Forms 6i n'est plus compatible avec le développement des outils technologiques et des produits ORACLE
- Des interfaces homme/machine qui ne sont pas pratiques.

Après avoir défini les problèmes de la solution actuelle BRSMCM, il reste à citer les différentes limitations et vulnérabilités de cette dernière, à savoir :

- La solution BRS MCM est développée sous oracle Forms 6i, donc plusieurs problèmes se posent hors de l'installation de l'application chez les clients : problème de performance.
- L'application est basée sur l'architecture client-serveur avec un client lourd ; les solutions client lourd sont également caractérisées comme étant des solutions très coûteuses tant au niveau de la maintenance que du déploiement et de la formation.
- Etant généralement installé sur le système d'exploitation de l'utilisateur, une nouvelle version doit être installée afin de la faire évoluer. Pour y remédier, les éditeurs de l'ancienne solution l'ont doté généralement d'une fonctionnalité exécutée au lancement de l'application, permettant de vérifier sur un serveur distant si une version plus récente est disponible et le cas échéant propose à l'utilisateur de la télécharger et de l'installer ce qui cause un grand échange de trafic sur le réseau intranet, ce qui influence la performance du réseau.
- Un grand problème de sécurité apparaît clairement ; lorsque l'application est installée chez un client, plusieurs fichiers contenant des informations sur l'authentification et l'accès aux bases de données sont laissées non cryptés sur les postes des utilisateurs, ce qui présente une grande faille dans la solution actuelle.
- Les fichiers XML générés par l'application BRSMCM et contenant des données confidentiels sont transmis en clair à BAM.

2.2. Expression du cahier des charges

La réalisation du projet BRSMCM exige des besoins à prendre en charge, des contraintes, des spécifications techniques et fonctionnelles à respecter et des règles de gestion à appliquer.

2.2.1. Spécifications fonctionnelles

Cette partie concerne l'expression fonctionnelle du besoin tel qu'exprimé par le client-utilisateur du produit: Il s'agit de mettre en évidence les fonctions de service ou d'estime du produit étudié ;

Les caractéristiques fonctionnelles du projet :

- **Chargement de données** : charger, par domaine, les flux sources conformément à l'entrée standard de BRSMCM dans l'entrepôt dédié au marché des changes et monétaire.
- **Gestion des flux du marché des changes** à savoir : la position de change, le change Spot, le change Terme, le Swap de devises, l'Option de change, l'encours global du portefeuille des options de change, l'encours détaillé du portefeuille des options de change, les prêts et emprunts en devises, les achats et ventes d'instrument financier à l'étranger, le change sur les produits de base ;il s'agit de la consultation et la gestion des données.
- **Gestion des flux du marché monétaire** à savoir : les prêts et emprunts en blanc, les opérations de pensions livrées, les opérations fermes du marché secondaire des BDT, les titres de créances négociables du marché primaire (TCN Primaire), les titres de créances négociables du marché secondaire (TCN Secondaire), l'encours des titres de créances négociables (Encours TCN), les dépôts à terme ; il s'agit de la consultation et gestion des données
- **Cours de devise** : Consultation et modification des cours de conversions de devise chargés sur l'entrepôt pour chaque date de déclaration.

- **Cours MID** : Consultation et modification des cours de conversions de devise MID chargés sur l'entrepôt pour chaque date de déclaration
- **Contrôle** : simuler, par domaine, le retour BAM via l'édition d'un rapport des anomalies éventuelles relevées sur la déclaration.
- **Gestion des fichiers XML** :
 - Génération, par domaine, d'un ou de la totalité des fichiers XML à destination de BAM.
 - consulter les fichiers et aller directement aux enregistrements comportant un retour négatif afin de les traiter et les recycler.
- **Liste des attributs** : Consulter et modifier les listes des attributs et des valeurs associées spécifiées par BAM pour la déclaration des données des marchés de change et monétaire.
- **Gestion des tiers** : consulter et gérer les informations des tiers chargées au niveau de l'entrepôt.

2.2.2. Les règles de gestion

Pour le marché des changes :

➤ **Les montants** :

- Les montants sont exprimés en dirhams.
- Les montants et contre-valeurs des montants sont des chiffres à 2 décimales et suivent la règle suivante de l'arrondi :
 - Si la 3ème décimale est 0, 1, 2,3 ou 4 alors ne rien ajouter à la 2ème décimale.
 - Sinon si la 3ème décimale est 5, 6, 7,8 ou 9 alors ajouter **1** à la 2ème décimale.

➤ **Les dates** :

- Les dates ont le format suivant : JJMMAAAA.
- La date de négociation \leq la date de valeur \leq la date d'échéance ou d'exercice.

- Pour les déclarations quotidiennes : La date de négociation, la date de la position de change ou la date d'évaluation = la date de déclaration.
- Pour la déclaration mensuelle « Encours détaillé des options de changes » :
 - La date de déclaration correspond au dernier jour ouvrable du mois à déclarer.
 - Les dates de négociations doivent être \leq la date de déclaration
 - Les dates d'échéance doivent être $>$ la date de déclaration.

➤ **Cours :**

- Le cours clôture MID BAM utilisé dans le calcul des contre-valeurs, doit avoir exactement 5 positions (sans la virgule). L'ajustement se fait au niveau des décimales et non pas au niveau de la part entière du cours, autrement dit :
 - Si le cours est <10 , il doit contenir exactement 4 décimales.
 - Si le cours est ≥ 10 et < 100 , il doit contenir exactement 3 décimales.
 - Si le cours est ≥ 100 , il doit contenir exactement 2 décimales...etc.
- Pour toutes les opérations **devise contre dirham** (devise cotée à l'incertain = MAD), le cours réel, le cours réel spot, le cours réel terme, le cours d'exercice et le cours spot à la souscription, doivent contenir exactement **4 décimales**.
- Il ne faut pas oublier de diviser par l'unité lorsque le cours devise contre dirham est renseigné avec une unité différente de 1. Un exemple : pour le Yen japonais, il faut renseigner le cours réel sans l'unité (9.8680) et pour la contre-valeur du montant en yen, il faut diviser par l'unité =100.

➤ **Contrepartie :**

- Si la catégorie des intervenants = 0 alors, la contrepartie correspond au Code SWIFT.
- Si la catégorie des intervenants =1 alors, la contrepartie correspond à la Raison sociale de l'intervenant.
- Si la catégorie des intervenants = 0X ou 1X alors, la contrepartie correspond à la raison sociale + le pays de résidence de l'intervenant.

- Si la catégorie des intervenants est 2 alors, la contrepartie est renseignée par **“PM”**.
- Si la catégorie des intervenants est 2X alors, la contrepartie est renseignée par **“PE”**.
- Pour les portefeuilles 1, 0X ou 1X, Il ne faut pas renseigner ni de code SWIFT, ni d’abréviations, ni de noms tronqués ou autres. Les sigles sont tolérés quand
- ils sont communément connus (pas de sigles de votre création. Par exemple, vous pouvez renseigner SG pour Société Générale).

➤ **Pourcentage :**

Les champs qui doivent être renseignés en pourcentage sont des chiffres à 3 décimales entre 0 et 1

➤ **Listes prédéfinies et autres :**

- Au niveau des déclarations, il faut renseigner le code et non pas le nom ou le libellé.
- Compte tenu du programme informatique développé pour traiter les déclarations des banques, il est impératif de ne pas renseigner « < » et « & » dans les éléments XML, surtout au niveau du champ **“Contrepartie”** lorsque le portefeuille = 1, 0X ou 1X et de manière générale, au niveau des champs libres.

Pour le marché monétaire :

➤ **Les montants :**

- Les montants sont exprimés en dirhams et en valeur absolue.
- Les montants et contre-valeurs des montants sont des chiffres à 2 décimales et suivent la règle suivante de l’arrondi :
 - Si la 3ème décimale est 0, 1, 2,3 ou 4 alors ne rien ajouter à la 2ème décimale.
 - Sinon si le 3ème décimale est 5, 6, 7,8 ou 9 alors ajouter **1** à la 2ème décimale.

➤ **Les dates :**

- Les dates ont le format suivant : JJMMAAAA

- La date de négociation est \leq la date de valeur ou date de cession ou date de jouissance $<$ la date d'échéance ou de rétrocession.
- Pour les déclarations quotidiennes, la date de déclaration est = la date de valeur ou de cession.
- Pour les déclarations hebdomadaires « TCN » (TCN Marché Primaire, TCN Marché Secondaire, Encours TCN) :
 - La date de déclaration correspond au dernier jour ouvrable de la semaine à déclarer
 - Les dates de jouissance doivent être comprises dans l'intervalle : [Premier jour ouvrable de la semaine à déclarer ; dernier jour ouvrable de la semaine à déclarer]
- La date de l'encours est égale à la date de déclaration (= correspond au dernier jour ouvrable de la semaine à déclarer)
- Pour la déclaration mensuelle « Dépôts à terme », la date de déclaration correspond au dernier jour ouvrable du mois.

➤ **Taux :**

- Le taux des opérations doit être déclaré en pourcentage avec exactement trois décimales (même si la 3ème décimale est = 0) et suit la règle suivante de l'arrondi :
 - Si la 4ème décimale est 0, 1, 2, 3 ou 4 alors ne rien rajouter à la 3ème décimale.
 - Sinon si la 4ème décimale est 5, 6, 7, 8 ou 9 alors rajouter 1 à la 3ème décimale.

➤ **Intervenants :**

- Si la catégorie des cédants, cessionnaires ou souscripteurs = 0 alors cédant, cessionnaire ou souscripteur = Code SWIFT
- Sinon ; le cédant, cessionnaire ou souscripteur = Raison sociale pour une personne morale et Identité pour une personne physique.
- L'établissement livreur (livré) est l'établissement déclarant dans le cas où

l'établissement livré (livreur) ne l'est pas. Toutefois, les établissements livreur et livré peuvent être tous les deux = à l'établissement déclarant.

- L'établissement emprunteur (prêteur) est l'établissement déclarant dans le cas où l'établissement prêteur (emprunteur) ne l'est pas. Toutefois, les établissements emprunteur et prêteur ne peuvent pas être tous les deux = à l'établissement déclarant.
- Si catégorie du titre = CD, alors Emetteur = code Swift, sinon Emetteur = Raison sociale.

➤ **Listes prédéfinies et autres :**

- Au niveau des déclarations, il faut renseigner le code et non pas le nom ou le libellé.
- Compte tenu du programme informatique développé pour traiter les déclarations des banques, il est impératif de ne pas renseigner « < » et « & » dans les éléments XML, surtout au niveau du champ "Contrepartie" lorsque le portefeuille = 1, 0X ou 1X et de manière générale, au niveau des champs libres.

2.2.3. Spécifications d'organisation et d'exploitation

- **Gestion des profils :** Créer les profils et de gérer les accès aux modules de BRSMCM. Chaque utilisateur sera affecté à un profil donné qui définira son accès à l'application.

Nous devons créer des différents profils et les affecter aux utilisateurs en leurs assignant des privilèges via des rôles, et il faut aussi éviter les rôles conflictuels.

- **Gestion des utilisateurs :** Saisir les utilisateurs de BRSMCM et leur affecter un profil :

Se connecter :

- L'utilisateur doit se connecter avant de pouvoir utiliser l'application intranet, il doit décliner son login et son mot de passe.

- Quels que soient les éléments intermédiaires de l'architecture technique ; il s'agira bien d'une authentification « de bout en bout » ; c'est-à-dire de la station de travail au serveur de traitements et données.
- Il ne doit y avoir qu'une seule connexion simultanée par utilisateur.

Se déconnecter :

- L'utilisateur doit pouvoir se déconnecter après avoir utilisé l'application intranet.
- L'utilisateur doit être déconnecté automatiquement s'il quitte le navigateur web sans terminer l'application ni se déconnecter volontairement, ou si le navigateur web se ferme brutalement suite à un dysfonctionnement interne.

Sécuriser la connexion :

- La confidentialité du mot de passe doit être assurée de bout en bout.
- Les tentatives de connexion avec un mot de passe erroné doivent être limitées à trois seuils au-delà duquel l'utilisateur doit être bloqué, il faudra disposer d'une fonction de déblocage.
- Les connexions et les tentatives infructueuses de connexions et de déconnexions doivent être tracées.

	A	B	C
1	Step 1: Role Names		
2			
3			
4			
5	New Role Name	Default Role Name	Description
6	Administrateur	Administrateur	ce profil permet l'accès uniquement au module d'administration (sécurité)
7	Exploitant	Exploitant	ce profil permet de faire tous les traitements au niveau de BRSMCM mais ne donne pas accès au référentiel sauf en mode « Consultation
8	Administrateur Fonctionnel	Administrateur Fonctionnel	ce profil donne accès juste au Référentiel de BRSMCM.

Figure 7 : Description des différents profils

6				
7	Role:	Administrateur		
8	Record Type	Has Access?	Can Create?	Can Read All Records?
9	Chargement			
10	Gestion des flux			
11	Archivage			
12	Cours de devise			
13	Cours MID			
14	Contrôles			
15	Génération fichier(s)XML			
16	Lecture fichier (s) retour BAM			
17	Lecture fichier (s)de retour Appariement			
18	Liste BAM			
19	Tiers			
20	Etablissement			
21	Flux			
22	Déclaration			
23	Options			
24	Gestion des profils	x	x	x
25	Gestion des utilisateurs	x	x	x

Figure 8 : Droits d'accès de l'administrateur aux modules de gestion des profils/utilisateurs

	Role:	Exploitant		
	Record Type	Has Access?	Can Create?	Can Read All Records?
	Chargement	x	x	x
	Gestion des flux	x	x	x
	Archivage	x	x	x
	Cours de devise	x	x	x
	Cours MID	x	x	x
	Contrôles	x	x	x
	Génération fichier(s)XML	x	x	x
	Lecture fichier (s) retour BAM	x	x	x
	Lecture fichier (s)de retour Appariement	x	x	x
	Liste BAM	x		
	Tiers	x		
	Etablissement	x		
	Flux	x	x	x
	Déclaration	x	x	x
	Options	x	x	x
	Gestion des profils			
	Gestion des utilisateurs			

Figure 9 : Droits d'accès de l'exploitant aux modules de contrôle et de traitement

35				
36	Role:	Administrateur Fonctionnel		
37	Record Type	Has Access?	Can Create?	Can Read All Records?
38	Chargement			
39	Gestion des flux			
40	Archivage			
41	Cours de devise			
42	Cours MID			
43	Contrôles			
44	Génération fichier(s)XML			
45	Lecture fichier (s) retour BAM			
46	Lecture fichier (s)de retour Appariement			
47	Liste BAM	X	X	X
48	Tiers	X	X	X
49	Etablissement	X	X	X
50	Flux			
51	Déclaration			
52	Options			
53	Gestion des profils			
54	Gestion des utilisateurs			

Figure 10 : Droits d'accès de l'administrateur fonctionnel au référentiel de BRS MCM

[illegible]

Figure 11 : Les rôles et les privilèges pour les utilisateurs

Les figures précédentes présentent une méthode d'organisation des rôles , privilèges et profils des utilisateurs qui vise à bien gérer les droits d'accès aux différents modules de la solution BRS MCM et séparer des rôles pour éviter l'affectation des rôles conflictuels aux utilisateurs[3].

Conclusion

Suite à cette phase d'expression des besoins fonctionnels du client il est désormais possible de réaliser une solution respectant les exigences fonctionnelles ainsi que les règles de gestion.

Nous devons nous assurer aussi de l'exécution de chacune des actions décrites .Il est aussi de notre obligation de permettre le suivi de toutes les étapes du processus par tous les acteurs impliqués, ces derniers sont avisés par un e-mail dès lors qu'ils sont assignés.

Dans le chapitre suivant nous allons appliquer la méthode de MEHARI (Méthode harmonisée d'analyse des risques) afin de faire une analyse des risques du projet, avant de présenter la conception de la nouvelle solution.

Analyse des risques et conception

Ce chapitre décrit l'application de la méthode harmonisée d'analyse des risques (MEHARI) pour l'analyse de risque de la solution et ce afin d'établir un plan d'actions.

Il s'agit ensuite d'identifier les interactions entre notre système et le monde extérieur afin de pouvoir délimiter le périmètre fonctionnel. La fin du chapitre est consacrée essentiellement à la présentation des différents diagrammes UML de scénarios et le diagramme d'activités qui illustrent la conception de la solution.

3. Analyse des risques et conception

3.1 . Analyse des risques

3.1.1. Introduction MEHARI

La méthode harmonisée d'analyse des risques (MEHARI) est conçue par le CLUSIF, et élaborée à partir d'autres méthodes (MARION et MELISA). Sa base de connaissance est évolutive, adaptable et ouverte vers les risques opérationnels et de métiers[4].

MEHARI permet de mettre en œuvre une politique globale de sécurité structurée par :

- Un plan stratégique,
- Des plans opérationnels,
- La construction des tableaux de bord.

MEHARI repose sur une logique des risques afin de mesurer sa gravité. Elle évalue :

- Les causes d'un sinistre, ou la potentialité d'un survenance
- Les conséquences, ou l'impact
- Les scénarios de sinistre ainsi obtenus couvrent notamment les domaines métiers et techniques

Il existe plusieurs démarches pour appliquer MEHARI, ces démarches sont les suivantes :

- Partir des enjeux majeurs, et analyser, pour chacun, comment il pourrait être attaqués, puis prendre les mesures en conséquence.
- Partir des vulnérabilités et les réduire toutes jusqu'à ce que les risques deviennent acceptable.

- Partir des situations de risque combinant les enjeux et les vulnérabilités et procéder à une analyse de risque .

La démarche MEHARI décrite dans la norme ISO/IEC est représentée schématiquement ci-dessous :

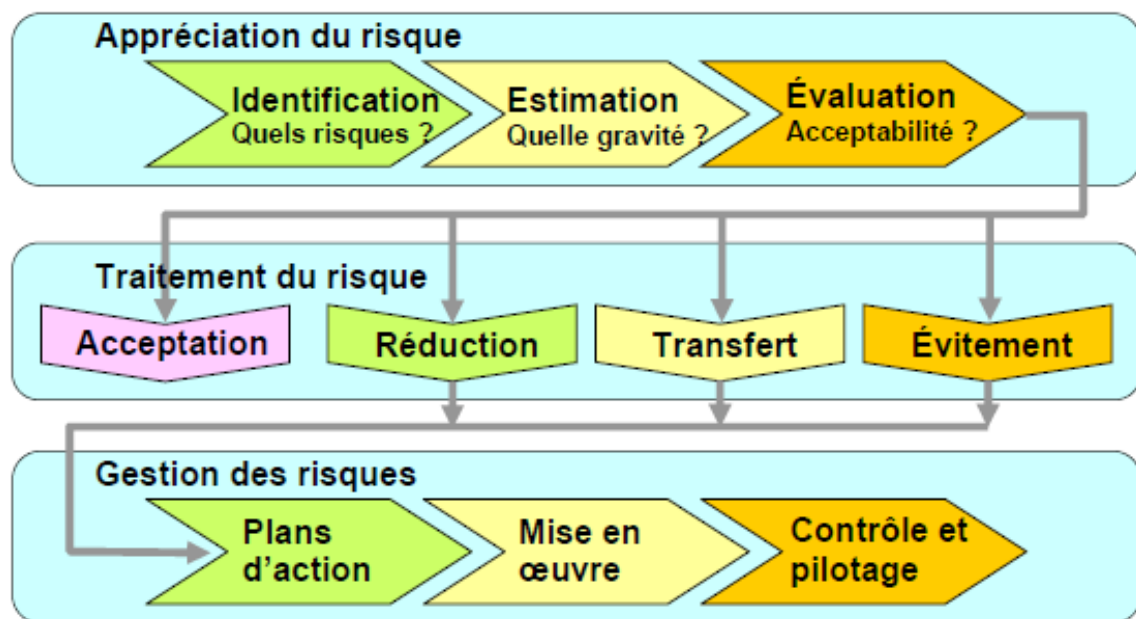


Figure 12 : Etapes dans la gestion des risques

Ce schéma fait apparaître trois grandes phases, les deux premières constituées de l'appréciation des risques et de l'élaboration des plans de traitement des risques correspondant à la phase planification « plan » de la norme ISO 27001 ,et une phase de mise en œuvre qui comprend elle-même , au sens de cette norme ,les aspects de déploiement « do »,de contrôle « check » ,et enfin d'amélioration et de correction éventuelle « act » .

Les différences principales entre les démarches adaptées à la gestion directe et individualisée des risques résident essentiellement dans la phase de planification, par la manière d'apprécier chaque risque et de définir le plan de traitement adapté à chacun.[5]

Le schéma suivant présente un résumé de l'utilisation de la démarche MEHARI :

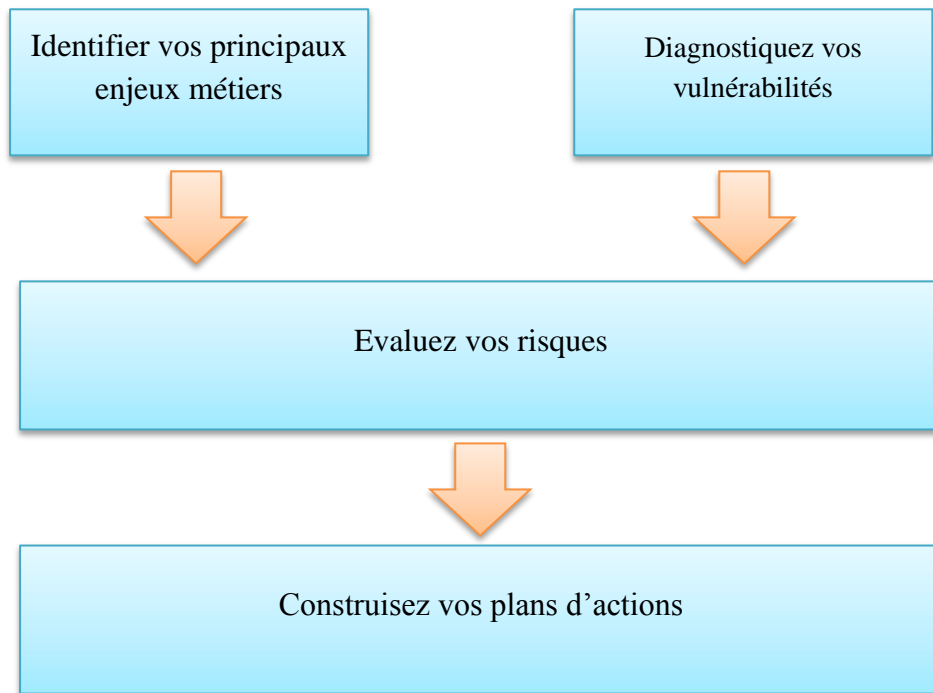


Figure 13 : Résumé de l'utilisation MEHARI

3.1.2. Analyse des enjeux et classification

La démarche MEHARI consiste à procéder à une analyse des activités et donc des processus de l'entreprise, de l'organisme ou du projet, d'en déduire les dysfonctionnements qui peuvent être redoutés, puis d'évaluer en quoi ces dysfonctionnements peuvent être plus ou moins graves, avant d'effectuer éventuellement, la classification proprement dites des actifs du projet selon le schéma [6] si dessous :

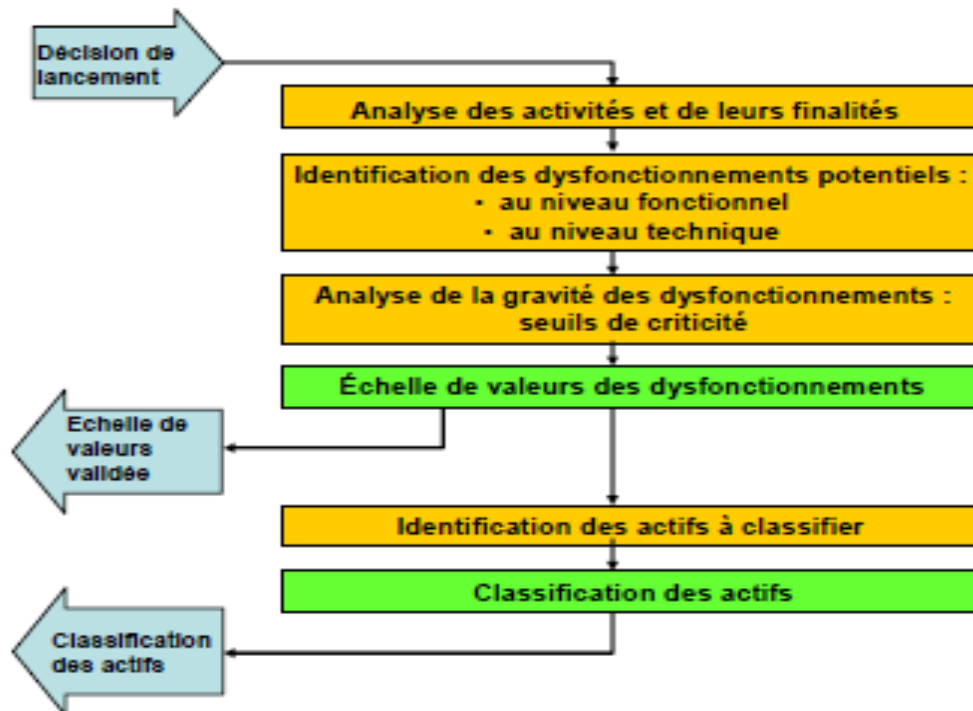


Figure 14 : Echelle de valeurs et classifications

➤ Analyse des enjeux de sécurité

- Identification des activités majeures du projet et de leurs finalités :

Fonctionnalités	Résultats attendus ou objectifs
Refonte de la solution BRS MCM sous Oracle APEX	Une nouvelle solution plus pratique
Administration des profils /utilisateurs	Séparation des rôles (éviter les rôles conflictuels) Assignation des privilèges aux utilisateurs pour assurer le contrôle d'accès

Tableau 4 : Activités majeurs du projet et leurs résultats attendus

- Identification des dysfonctionnements redoutés :

Dysfonctionnement	Conséquences
Fichiers de données indisponibles ou contenant des données erronées	Problèmes de chargement de données et de génération des fichiers XML
Accès non autorisé aux bases de données	Lecture/Ecriture non autorisée des tables ou procédures
Accès intranet non disponible	Pas d'accès à l'application web

Tableau 5 : Identification des dysfonctionnements redoutés

- Evaluation de la gravité des dysfonctionnements identifiés :

Dysfonctionnement	Niveau 1 Non significatif	Niveau 2 Important	Niveau 3 Grave	Niveau 4 Vital
Fichiers de données indisponibles ou contenant des données erronées	Données indisponibles pour moins que 2 heures	Données indisponibles ou erronées entre 2 et 4 heures	Indisponibilité des données pour plus que 4 heures	
Accès non autorisé aux bases des données	Lecture des données qui ne sont pas critiques	Lecture des données critiques	Lecture et modification des données	
Accès intranet non disponible	Problèmes d'accès au réseau pour une durée moins d'une heure	Problèmes d'accès au réseau pour une durée entre une et deux heures	Problèmes d'accès au réseau pour une durée plus que deux heures	

Tableau 6 : Evaluation de la gravité des dysfonctionnements identifiés

➤ **Analyse des risques : Classification**

- **Objectifs :**

Déterminer la sensibilité de chaque classe d'actifs, sous forme d'une classification.

Les classes d'actifs utilisées par la base de connaissances de MEHARI 2010 sont des regroupements, par domaine d'activité, des types d'actifs primaires.

La classification est à faire avec un niveau de 1 à 4 pour les critères de Disponibilité, d'Intégrité, de Confidentialité et d'Efficiency exigée.

La classification a pour objectif de remplir les tableaux de classification **T1**, **T2** et **T3** de la base de connaissance ainsi qu'indiqué dans le document « *Méhari 2010 – Guide de l'analyse des enjeux et de la classification* ». Chaque cellule de ce tableau devra ainsi indiquer le degré maximal de gravité que pourrait représenter le dommage subi suite à la perte de disponibilité, d'intégrité ou de confidentialité pour ce type d'actif ou pour le non-respect de l'exigence d'efficacité vis à vis d'une loi ou d'une réglementation, pour l'activité concernée (précisée sur chaque ligne des tableaux)

- **Acteurs et parties permanentes :**

L'animateur de la tâche est le responsable de la mission d'analyse et de traitement des risques.

Sont parties prenantes :

- Les responsables d'activité
- La DSI
- Le RSSI
- La Direction juridique (pour le tableau T3)

- **Livrables :**

Les livrables sont constitués des tableaux de classification T1, T2 et T3.

- **Processus :**

Le processus, qui est décrit dans le « *guide de l'analyse des enjeux et de la classification* », comprend les éléments suivants :

➤ Indication, dans les tableaux T1 et T2, des processus correspondant aux divers domaines d'activité pris en compte lors de l'élaboration de l'échelle de valeur des dysfonctionnements.

➤ Remplissage de ces 2 tableaux, par domaine d'activité, et cellule par cellule :

Chaque cellule ou case du tableau représentant le niveau du dommage subi suite à la perte de disponibilité, d'intégrité ou de confidentialité) par un type d'actif (indiqué en tête de colonne), pour une activité donnée (précisée sur chaque ligne du tableau), On recherchera :

- Si ce dommage peut conduire à un ou plusieurs dysfonctionnements indiqués dans l'échelle de valeur des dysfonctionnements.
- Si tel est le cas, quel niveau d'impact maximal peut être atteint et ce niveau constituera alors la classification à reporter dans la cellule du tableau.
- Si tel n'est pas le cas, un 1 (plus faible niveau d'impact) sera reporté dans la cellule du tableau.

➤ Indication dans le tableau T3, qui comporte une colonne pour chaque exigence indiquée en tête de colonne (E pour Efficience), du niveau d'impact qu'aurait une non-conformité pour chacun des processus métier et transversaux cités. Ceci est à faire avec les responsables d'activité assistés de la Direction Juridique et de la Direction de la Communication.

➤ Remplissage, sur le même principe, des lignes des 3 tableaux correspondant à la prise en compte des processus transversaux s'ajoutant aux processus propres à chaque activité métier (qui peuvent indiquer un impact plus important que la synthèse des besoins de chaque activité métier)

➤ Validation en Comité de Direction

- **Identification des actifs :**

Dans le tableau qui suit, nous avons énuméré les différentes catégories d'actifs sur lesquelles nous avons mené notre analyse de risques liées aux données du projet BRS MCM.

- Fichiers de données ou bases de données applicatives

- Données applicatives isolées, en transit messages

- Fichiers bureautiques partagés

- Listings ou états imprimables

- Archives informatiques

- Données et informations publiées (web ou internet)

Tableau 7 : Actifs de type données et informations

Les figures suivantes présentent la classification des actifs du périmètre sur lequel nous allons appliquer MEHARI est qui est le projet de refonte de la solution BRS MCM.[7]

A	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	A
Tableau T1	CLASSIFICATION DES DONNÉES																													
Processus métier, domaine applicatif ou domaine d'activité Services communs à particulariser	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		Archives informatiques		Données publiées (web ou interne)					
	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	In
Projet de refonte de la solution BRSMCM	4	3	2	3	2	1	3	3	1						2								2	1	1	3	3	2		1
Administration/ politique d'ensemble				3	3												2		2											1
Classification pour l'ensemble	4	3	3	3	2	1	3	3	1						2		2		2				2	1	1	3	3	2		
Classification pour le périmètre choisi	4	3	3	3	2	1	3	3	1						2		2		2				2	1	1	3	3	2		

Figure 15 : Tableau T1 classification des actifs de catégorie « données »

Tableau T2	CLASSIFICATION DES SERVICES																	
Processus métier, application ou domaine applicatif Services communs	Services du réseau étendu		Services du réseau local		Services applicatifs			Services bureautiques communs		Equipements 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	
Projet de refonte de la solution BRSMCM	3	2	3	1	3	2	2			2			2	3		1	1	
Classification pour l'ensemble	3	2	3	3	3	2	2			2			2	3		1	1	
Classification pour le périmètre	3	2	3	3	3	2	2			2			2	3		1	1	

Figure 16 : Tableau T1 classification des actifs de catégorie « Services »

1	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
2			E	E	E	E	E	E
3								
5	Processus métiers							
6	Projet de refonte de la solution BRSMCM				2		3	3
7	Administration/ politique d'ensemble				3	3		
8								
9	Classification pour l'ensemble				3	3	3	3

Figure 17 : Tableau T3 classification des actifs « processus de management »

3.1.3. Elaboration du plan d'actions

Après avoir fait une analyse des enjeux de la sécurité et une classification, nous avons déduit plusieurs scénarios de risques (Annexes A et B) ; donc il faut établir un plan d'action efficace et rapide afin de minimiser les risques graves et éliminer certains parmi eux.

L'élaboration du plan d'actions doit respecter le manuel de référence des services de sécurité de MEHARI.

Ce manuel [8] fournit par ailleurs des apports directement utilisables pour proposer des améliorations de sécurité « ponctuelles » ou à apporter à la politique de sécurité, sinon pour rédiger un tel document. Cette prestation de MEHARI permet d'obtenir directement plusieurs types d'indicateurs de sécurité globaux : associés à des services ou domaines de sécurité ou à des thèmes transversaux (contrôles d'accès, plans de continuité d'activité, etc.) ou aux contrôles recommandés par la norme ISO/IEC 27002/27005.

Plusieurs scénarios doivent s'appliquer afin de minimiser les risques établis par l'analyse des enjeux et la classification :

➤ **Contrôle de la mise en production de nouveaux systèmes ou d'évolutions des systèmes existants :**

- **Objectif :**

Gérer avec rigueur les problèmes de sécurité que peut poser la mise en production de nouveaux systèmes (matériel, logiciel opératoire, middleware, applicatif) ou de nouvelles versions de systèmes existants.

- **Résultats attendus :**

Éviter que la mise en production de nouveaux systèmes (matériel, logiciel opératoire, middleware, applicatif) ou de nouvelles versions de systèmes existants n'ouvre une faille de sécurité non suspectée (nouvelle faille ou faille connue dont la correction pourrait être inhibée par la nouvelle mise en production).

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont essentiellement de nature organisationnelle.

Mesures organisationnelles :

Le problème que peuvent poser, du point de vue de la sécurité, ces installations de systèmes tient au fait que les équipes d'exploitation n'ont pas forcément les outils ni la formation pour envisager les risques pouvant être créés par ces installations ou évolutions. Les mesures à mettre en œuvre sont de plusieurs ordres :

- Etablissement de procédures formelles de décision, d'approbation et de contrôle préalable aux décisions d'installation ou de changement d'équipements et de versions tenant compte des exigences de sécurité physique et logique ainsi que celles émises par les utilisateurs.
- L'analyse des nouvelles fonctionnalités et des risques nouveaux éventuels, de même que pour un nouveau projet : Analyse des risques que ces nouvelles fonctionnalités peuvent induire ou faciliter.
- La vérification que les paramétrages et dispositifs de sécurité prévus sur les versions précédentes, en cas d'évolution, sont bien toujours en place et actifs.

Mesures techniques :

Les mesures techniques d'accompagnement dépendent pour une grande part des décisions prises à la suite de l'analyse de risque décrite ci-dessus.

- **Qualité de service :**

- L'efficacité du service est essentiellement liée à la rigueur de l'analyse menée à l'occasion de l'installation ou de l'évolution et, en particulier : au formalisme de l'analyse de risque et des conclusions qui en sont tirées, à la formation préalable des équipes d'exploitation à ce type de démarche.
- La robustesse du service est liée à la volonté de la Direction de ne pas déroger aux procédures formelles d'analyse de risque et de contrôle de conformité sauf circonstances réellement exceptionnelles et au formalisme rigoureux alors nécessaire (signature formelle d'une dérogation par un membre de la Direction). La principale cause de contournement vient, en effet, de la tendance à déroger aux procédures d'analyse de risque ou de contrôle de conformité sous la pression des délais.

➤ **Authentification et contrôle des droits d'accès des administrateurs et personnels d'exploitation :**

- **Objectifs :**

S'assurer lors de l'accès aux systèmes d'information avec des droits privilégiés que la personne qui tente de se connecter est bien celle qu'elle prétend être.

- **Résultats attendus :**

Prévenir les actions néfastes pouvant être menées, volontairement ou non, par des personnes n'étant pas (ou plus) autorisées individuellement à accéder aux systèmes avec des droits privilégiés.

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont essentiellement techniques, mais s'appuient également sur des mesures organisationnelles.

Mesures techniques :

- Les mesures techniques de base concernent le contrôle des droits d'accès d'une part et l'authentification d'autre part, c'est-à-dire le contrôle d'une caractéristique que la personne, individuellement, possède ou connaît :
Vérification des droits d'accès en fonction du contexte d'accès (local ou à distance, par lien sécurisé ou non, horaire, etc.), le contrôle du mot de passe ou du secret partagé entre la personne et un équipement de contrôle, le contrôle d'un objet physique reconnaissable possédé par la personne (généralement en association avec un secret partagé entre la personne et l'objet)
- Les mesures complémentaires concernent la protection contre les tentatives d'usurpation d'identité : Protection du processus de diffusion initiale des conventions secrètes (mots de passe), Protection du protocole d'authentification pour éviter qu'il ne soit écouté et dupliqué, Protection des éléments d'authentification conservés par l'utilisateur ou les équipements assurant l'authentification (stockage des mots de passe, par exemple), Inhibition du processus d'authentification en cas de tentative répétée infructueuse.

Mesures organisationnelles d'accompagnement :

Les mesures organisationnelles d'accompagnement concernent la gestion des anomalies ou des dysfonctionnements ou violations des mesures techniques :

- Gestion de relation utilisateur en cas de perte de mot de passe ou de support d'authentification.
- Procédures d'alerte en cas de tentatives répétées échouées.
- **Qualité de service :**
 - L'efficacité du service est liée à la solidité ou l'inviolabilité du mécanisme d'authentification proprement dit (force et solidité du moyen d'authentification, solidité de l'algorithme cryptologique éventuellement utilisé pour authentifier, solidité de l'algorithme et du protocole contre toute écoute et réutilisation de séquence, etc.)

- La mise sous contrôle est réalisée par des audits réguliers :
 - Des profils et des droits privilégiés ainsi que leur attribution à ces personnes
 - Des paramètres supports des mécanismes d'authentification,
 - Des systèmes de détection des violations et des arrêts du contrôle d'accès
 - Des procédures de réaction aux anomalies et incidents et de la mise en œuvre de ces procédures.

➤ **Sauvegarde des données applicatives :**

- **Objectif :**

Organiser la sauvegarde des données relatives aux applications.

- **Résultats attendus :**

Permettre une reprise rapide de l'exploitation des applications en cas d'incident, de reconfiguration de systèmes ou de mise en œuvre de plans de secours.

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont à la fois organisationnels et techniques.

Mesures organisationnelles

- Les mesures organisationnelles de base visent à planifier et organiser les sauvegardes des données applicatives en fonction de deux aspects également importants :
 - L'étude de la durée maximale admissible entre deux sauvegardes pour que les inconvénients subis par les utilisateurs soient acceptables
 - Le synchronisme entre fichiers sauvegardés pour assurer que l'exploitation des applications puisse effectivement reprendre avec les données sauvegardées, en toute cohérence.
- Les mesures organisationnelles d'accompagnement visent à s'assurer que les sauvegardes pourront être utilisées :
 - Contrôles de relecture périodiques
 - Test effectif que l'on peut redémarrer les applications et les services correspondants à partir des sauvegardes

- **Qualité de service :**

- L'efficacité du service est essentiellement liée à deux facteurs :
 - La fréquence des sauvegardes et son adéquation aux besoins des utilisateurs
 - Le synchronisme de sauvegardes
 - L'automatisation des opérations de sauvegardes proprement dites
- La robustesse du service est liée à plusieurs types de facteurs :
 - La protection des automatismes contre toute altération ou modification non contrôlée
 - L'externalisation de sauvegardes de recours
- La mise sous contrôle est réalisée par :
 - Des essais réguliers de relecture des sauvegardes des données applicatives
 - Des tests effectués pour vérifier que l'on peut effectivement, à partir des sauvegardes, restaurer complètement les applications et redémarrer un service effectif.

➤ **Contrôles permanents sur les données :**

- **Objectif :**

Protéger l'intégrité des données par des contrôles applicatifs sur les données elles-mêmes.

- **Résultats attendus :**

Empêcher qu'une erreur ou qu'une malveillance, dans la saisie des données ou dans des processus opératoires, se propage et se traduise par une pollution incontrôlée de bases de données.

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont essentiellement organisationnels, mais s'appuient sur des mesures techniques :

Mesures organisationnelles :

Les mesures organisationnelles de base consistent à définir un contrôle de la pertinence des données, en les comparant à des ratios ou des fourchettes de

vraisemblance, en faisant des contrôles de cohérence par rapport à des valeurs passées ou à d'autres données, etc. Des exemples types sont que la masse salariale ne dépasse pas une valeur donnée, que le même compte bancaire n'est pas présent dans une bande de virement de salaires plus de 5 fois, qu'un virement ne dépasse pas tel plafond, etc.

Les mesures organisationnelles d'accompagnement consistent à définir les actions à mener en cas de détection d'une anomalie par les contrôles (blocage de la transaction en cours, alerte, etc.).

Mesures techniques :

Les mesures techniques d'accompagnement visent à incorporer ces contrôles dans le code des applications et ceci de manière contrôlable :

- Identification des parties de code correspondant à des contrôles, pour qu'elles soient audibles.
- Séparation des paramètres de contrôle du code même de contrôle.
- **Qualité de service :**
 - L'efficacité du service est essentiellement liée à :
 - La rigueur de l'analyse ayant conduit à introduire des contrôles permanents
 - L'étroitesse des fourchettes de contrôle
 - La robustesse du service est liée à la protection du système de contrôle :
 - Protection du code contre toute altération ou inhibition
 - Protection des tables de contrôle contre toute modification induite
 - La mise sous contrôle est réalisée par des audits réguliers :
 - De la pertinence des paramètres de contrôle,
 - Du processus de contrôle

➤ **Protection de la confidentialité des données contenues sur le poste de travail ou sur un serveur de données (disque logique pour le poste de travail) :**

- **Objectif :**

Contrôler l'accès en lecture aux données pouvant résider sur le poste de travail.

- **Résultats attendus :**

Éviter que les personnes pouvant avoir accès au poste de travail puissent prendre connaissance des données qu'il contient ou qu'il a contenues :

- Fichiers vivants
- Fichiers effacés
- Fichiers temporaires

Le service vise également à se protéger contre des accès aux informations par des administrateurs de postes de travail.

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont à la fois techniques et organisationnels.

Mesures techniques :

Les mesures techniques sont de différentes natures selon la nature des fichiers que l'on souhaite protéger :

- Chiffrement des fichiers vivants
- Effacement réel et fiable des fichiers et informations inutiles
- Effacement réel et fiable des fichiers temporaires

Mesures organisationnelles :

De tels systèmes ne peuvent être mis en œuvre sans des mesures de sensibilisation et de formation du personnel pour qu'il comprenne bien ce qu'il convient de faire :

- Le chiffrement des fichiers est certes utile, mais, quand on utilise ces fichiers, ils sont alors « en clair » et cela demande des procédures particulières. Par ailleurs, si le chiffrement n'est pas déclenché par directory, il faut le faire manuellement et donc y prendre garde (en particulier pour les pièces jointes de messages ou les adresses de messagerie – risque de modification insoupçonnée qui peuvent être stockées sur un directory non chiffré et qu'il faut donc chiffrer volontairement ou ranger dans un directory chiffré).

- L'effacement réel des fichiers est possible par certains produits, mais il faut le plus souvent les activer spécialement et à chaque effacement réel
- L'effacement des fichiers temporaires peut également être programmé, mais il ne sera réel, le plus souvent, qu'à la fermeture du système.

En fonction des remarques qui viennent d'être faites, des directives précises sont un doivent couvrir les divers points cités (fichiers, messages, adresses de messagerie, fichiers détruits, fichiers temporaires, etc.)

- **Qualité de service :**

- L'efficacité du service est liée à :
 - L'exhaustivité des fonctions prévues
 - La solidité des mécanismes mis en place (en particulier chiffrement et effacement)
 - La sensibilisation des utilisateurs
 - La robustesse du service est liée à :
 - La protection du processus de mise en œuvre du déchiffrement ou d'effacement
 - La sécurité du processus de distribution des clés de chiffrement.
- La mise sous contrôle est réalisée par des audits réguliers :
 - De la mise à disposition réelle des utilisateurs des solutions préconisées (avec le support correspondant)
 - De l'usage, par les utilisateurs, des solutions offertes

- **Surveillance en temps réel du réseau étendu :**

- **Objectifs :**

Détecter en temps réel des anomalies de comportement ou des séquences anormales significatives d'actions non autorisées et potentiellement dangereuses sur le réseau étendu

- **Résultats attendus :**

Permettre une réaction rapide et, si possible, une intervention avant que l'action nocive ait été réussie. A défaut limiter cette action dans le temps (dans certains cas d'intrusion, on est surpris de constater que des traces existaient depuis fort longtemps et auraient permis de réagir).

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont à la fois techniques et organisationnels

Mesures techniques :

Les mesures techniques comportent deux types de solutions :

- Les systèmes de détection d'intrusion qui s'appuient sur des bases de données de séquences révélatrices de tentatives d'intrusion.
- L'enregistrement de rejets opérés par les systèmes de filtrage et la détection de répétitions anormales de rejets (tentatives de connexion avortées, rejets de protocoles et tentatives successives de différents protocoles, etc.)

Ces systèmes, qui peuvent être supportés par des outils plus ou moins sophistiqués, débouchent sur des alertes à destination d'une équipe d'intervention, voire sur des actions automatiques (blocage de la connexion, blocage de toutes les connexions en cas d'attaque en déni de service, etc.).

Il est clair qu'en accompagnement de ces mesures, les droits d'administration nécessaires pour paramétrer ces systèmes doivent être strictement contrôlés.

Mesures organisationnelles :

Les mesures organisationnelles de base visent à supporter les mesures techniques :

- mise à jour régulière de la base de données des techniques d'intrusion
- gestion des paramètres de détection des répétitions déclenchant une alarme.

En amont de ces mesures, il est nécessaire d'analyser tous les cas d'alerte et de définir, cas par cas, les réactions attendues de l'équipe d'intervention.

En complément, il peut être souhaitable d'analyser, en fonction du contexte de l'entreprise, si des comportements particuliers pourraient être significatifs d'actions anormales et donner lieu à une alerte spécifique, par exemple :

- Les horaires de connexion
- Les actions menées depuis des sites particuliers
- La multiplication des accès vers des sites distants

- **Qualité de service :**

L'efficacité du service est liée à plusieurs facteurs :

- le nombre de cas détectés et la profondeur de l'analyse préliminaire des cas donnant lieu à alarme, ainsi que le maintien à jour de ces données

- la qualité et la rigueur de l'analyse des réactions attendues de l'équipe d'intervention
- la compétence de cette équipe et sa disponibilité

La robustesse du service est liée à deux facteurs :

- La rigueur de la gestion des droits nécessaires pour administrer les paramètres d'alarmes et la solidité des contrôles qui sont faits à ce sujet
- L'alerte directe de l'équipe d'intervention en cas d'inhibition ou d'arrêt du système de surveillance

La mise sous contrôle est réalisée par des audits :

- Du bon fonctionnement du système de surveillance
- De la disponibilité de l'équipe d'astreinte et de la surveillance effective du réseau.

➤ **Contrôle de la mise en production de nouveaux logiciels ou matériels ou d'évolutions de logiciels ou matériels :**

- **Objectifs :**

Gérer avec rigueur les problèmes de sécurité induits par la mise en production de nouveaux équipements (matériel, logiciel opératoire ou applicatif) ou de nouvelles versions d'équipements existants.

- **Résultats attendus :**

Éviter que la mise en production de nouveaux équipements de réseau (matériel, logiciel opératoire, logiciel applicatif) ou de nouvelles versions d'équipements de réseau existants n'ouvre une faille de sécurité non suspectée (nouvelle faille ou faille connue dont la correction pourrait être inhibée par la nouvelle mise en production).

- **Mécanismes et solutions :**

Les mécanismes à mettre en œuvre sont essentiellement de nature organisationnelle.

Mesures organisationnelles :

Le problème que peuvent poser, du point de vue de la sécurité, ces installations d'équipements ou de systèmes tient au fait que les équipes d'exploitation n'ont pas

forcément les outils ni la formation pour envisager les risques pouvant être créés par ces installations ou évolutions. Les mesures à mettre en œuvre sont de trois ordres :

- Établissement de procédures formelles de décision, d’approbation et de contrôle préalable aux décisions d’installation ou de changement d’équipements et de versions tenant compte des exigences de sécurité physique et logique ainsi que celles émises par les utilisateurs.
- Analyse des nouvelles fonctionnalités et des risques nouveaux éventuels, comme pour un nouveau projet :
 - Identification des nouvelles fonctionnalités apportées par la mise en production projetée.
 - Jugement sur le caractère acceptable ou non de ces risques nouveaux
 - Prise de décision sur les mesures complémentaires éventuelles à mettre en œuvre.
- Vérification que les paramétrages et dispositifs de sécurité prévus sur les versions précédentes, en cas d’évolution, sont bien toujours en place et actifs :
 - Tenue à jour d’une liste des paramètres de sécurité et des points de contrôle.
 - Vérification du suivi des procédures et de l’activation de tous les processus de sécurité.

Mesures techniques :

Les mesures techniques d’accompagnement dépendent pour une grande part des décisions prises à la suite de l’analyse de risque décrite ci-dessus.

- **Qualité de service :**

- L’efficacité du service est essentiellement liée à la rigueur de l’analyse menée à l’occasion de l’installation ou de l’évolution et, en particulier :
 - Au formalisme de l’analyse de risque et des conclusions qui en sont tirées
 - Aux capacités de support de la part d’une cellule spécialisée
 - À la formation préalable des équipes d’exploitation à ce type de démarche.

- Au formalisme attaché aux tests de sécurité, à la tenue à jour des paramétrages de sécurité de chaque équipement et du contrôle de conformité de ces paramètres sur une nouvelle version.
- La robustesse du service est liée à :
 - La volonté de la Direction de ne pas déroger aux procédures formelles de mise en production sauf circonstances réellement exceptionnelles et au formalisme rigoureux alors nécessaire (signature formelle d'une dérogation par la Direction). La principale cause de contournement vient, en effet, de la tendance à déroger aux procédures d'analyse de risque ou de contrôle de conformité sous la pression des délais.
 - L'impossibilité de procéder à des mises production pour du personnel n'ayant pas cette fonction et à la solidité des contrôles correspondants (rigueur dans l'attribution des profils et authentification forte)

Après avoir établi le plan d'actions à suivre pour minimiser les risques et garantir la réalisation d'une solution fiable et performante il est à présent temps de passer à la conception de la nouvelle solution.

3.2. Conception

3.2.1. Présentation du langage UML

« *Unified Model Language* » comme son nom l'indique est un langage capable de modéliser un système basé sur des concepts orientés objets. Il unifie et formalise les méthodes pour des approches orientées objets [9].

Le langage UML est venu pour répondre à un besoin de conformité client et livrable. L'UML permet au-delà de la modélisation et la compréhension de résoudre les problèmes liés au besoin d'analyse en mettant en un ensemble de documents permettant une meilleure facilité de compréhension et une mise en place fidèle lors de l'implémentation.

UML est un langage basé sur les diagrammes. Un diagramme UML est une représentation graphique, qui s'intéresse à un aspect précis du modèle ; c'est une perspective du modèle.

Vu que l'application doit être robuste, extensible et modulaire, une modélisation objet apparaît la plus adaptée. En effet, l'objet a fait ses preuves dans la réalisation d'applications temps réel. C'est pourquoi j'ai opté pour UML comme langage de modélisation. Ce choix peut être justifié également par plusieurs raisons :

La notation UML facilite la compréhension et la communication d'une modélisation objet.

- La notation UML, par définition, n'est pas spécifique à un langage de programmation objet, elle peut donc être utilisée avec n'importe quel langage tel que C#, J#, JAVA ou C++.
- UML est aujourd'hui un standard, adopté par les grands constructeurs de logiciel du marché dont Microsoft.

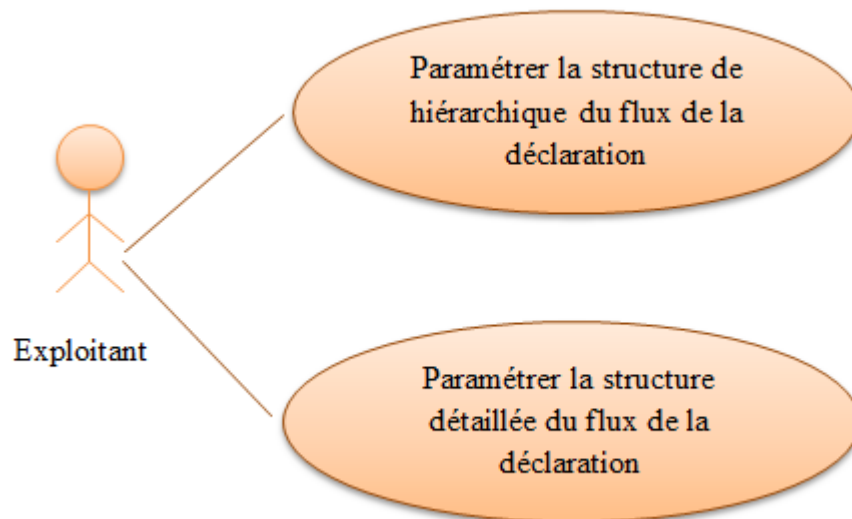
Durant notre étude du système, j'ai utilisé trois diagrammes de UML, il s'agit du diagramme des cas d'utilisation, les diagrammes de séquences, et le diagramme de déploiement.

3.2.2. Identification des cas d'utilisation

Comme il s'agit d'une application Web, il aura deux acteurs qui sont l'utilisateur de l'application et l'administrateur, Le diagramme que nous allons présenter par la suite montre les interactions entre les cas d'utilisation et l'utilisateur du système.

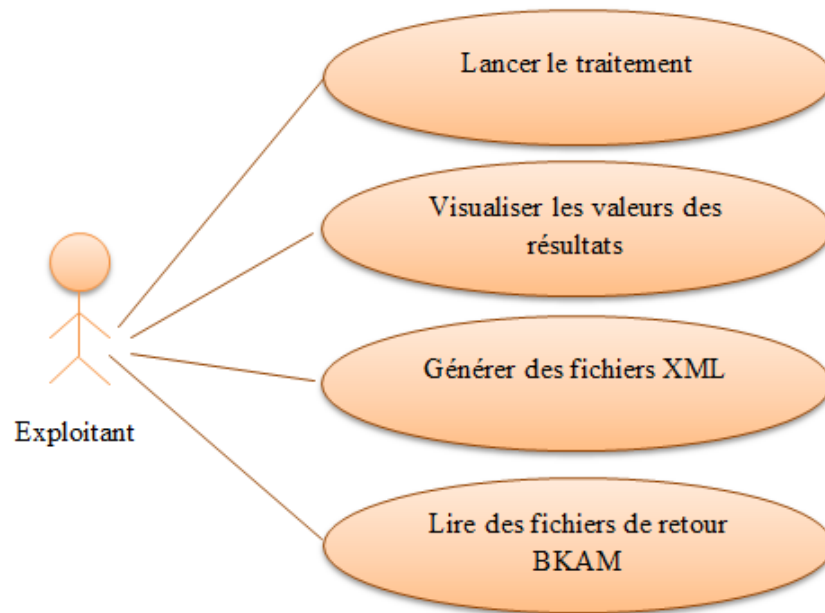
En afin de simplifier le digramme de cas d'utilisation en les a diviser a trois packages.

- Paramétrage
- Traitement
- Sécurité
- Gestion du référentiel

a) Package 1 : Paramétrage**Figure 18 : Cas d'utilisation du package paramétrage**

Ce diagramme représente la partie paramétrage de l'application et plus précisément les fonctionnalités suivantes :

- Paramétrer la structure de hiérarchique du flux de la déclaration : paramétrer, d'une façon complète, la structure de la déclaration (entête et contenu), les contrôles (format, longueur, obligatoire/optionnel, listes de valeurs..etc), ainsi que toutes les règles de gestion spécifiées par BAM sur les champs de la déclaration.
- Paramétrer la structure détaillée du flux de la déclaration : spécifier les types de compartiments, la structure de la déclaration et les règles de contrôle.

b) Package 2 : Traitement**Figure 19 : Cas d'utilisation du package traitement**

Ce diagramme représente la partie paramétrage de l'application et plus précisément les fonctionnalités suivantes

- Lancer traitement : l'utilisateur est amené à saisir des données en entrées à savoir :
 - ✓ La date de déclaration
 - ✓ L'établissement
 - ✓ La version

Une fois toutes ces données entrées et vérifiées on procède au lancement du traitement.

- Visualiser les valeurs des résultats : Elle permet d'afficher le résultat du traitement sous forme de valeurs retournées par chaque domaine.

- Générer les fichiers XML : les résultats des traitements sont envoyés à BAM sous le format XML, le chemin d'accès à ces fichiers s'affiche sur l'écran.
- Lire les fichiers de retours BAM : consulter les résultats sur un écran dédié de la solution et aller directement aux enregistrements comportant un retour négatif afin de les traiter et les recycler.

c) Le package : Sécurité

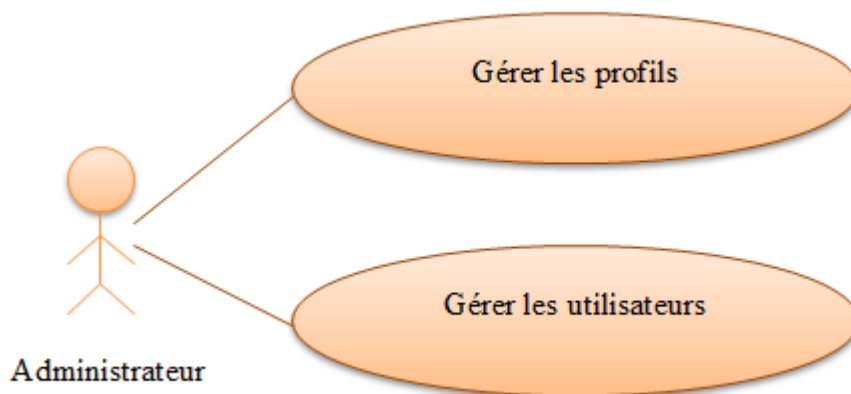
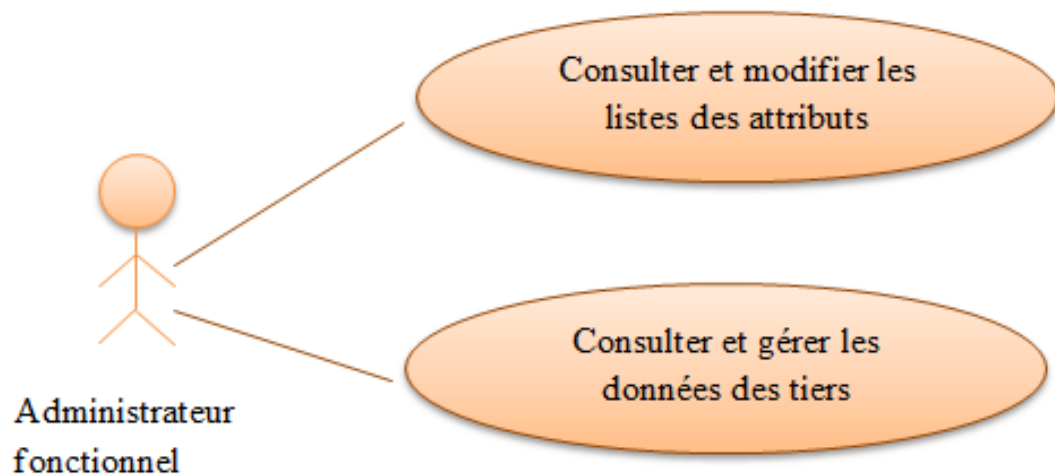


Figure 20 : Cas d'utilisation du package sécurité

Ce diagramme représente la partie sécurité de l'application et plus précisément les fonctionnalités suivantes :

- La gestion des utilisateurs : La création d'un nouvel utilisateur, la modification et la suppression.
- La gestion des profils : Cette partie est relative à l'attribution des droits de chaque utilisateur pour déterminer les privilèges dont il disposera par exemple :
 - Administrateur
 - Exploitant
 - Administrateur fonctionnel

d) Package 4 : Gestion du référentiel**Figure 21 : Cas d'utilisation de gestion du référentiel**

- Consulter et modifier la liste des attributs : consulter et modifier les listes des attributs et des valeurs associées spécifiées par BAM pour la déclaration des données des marchés de change et monétaire.
- Consulter et gérer les données des tiers : spécifier le nom, le code, l'adresse et toute autre information sur le client.

On peut rassembler ces 4 packages dans un seul diagramme de cas d'utilisation pour avoir une vue globale sur l'ensemble des fonctionnalités de l'application comme démontré dans la figure suivante :

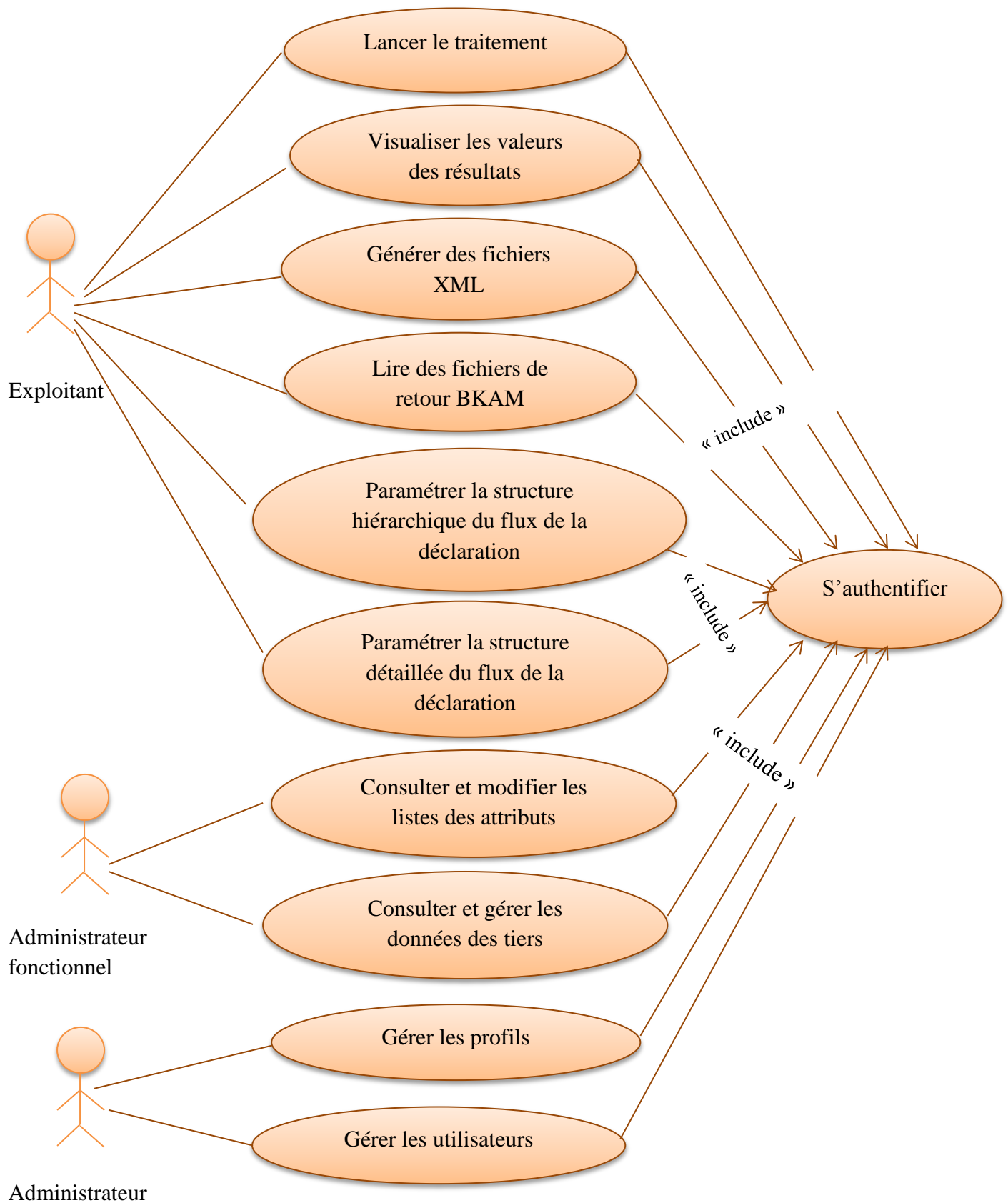


Figure 22 : Diagramme de cas d'utilisation général

3.2.3. Diagramme de classe

Le diagramme de classes est un schéma utilisé en génie logiciel pour présenter les classes et les interfaces des systèmes ainsi que les différentes relations entre celles-ci. Ce diagramme fait partie de la partie statique d'UML car il fait abstraction des aspects temporels et dynamiques.

Une classe décrit les responsabilités, le comportement et le type d'un ensemble d'objets. Les éléments de cet ensemble sont les instances de la classe.

Une classe est un ensemble de fonctions et de données (attributs) qui sont liées ensemble par un champ sémantique. Les classes sont utilisées dans la programmation orientée objet. Elles permettent de modéliser un programme et ainsi de découper une tâche complexe en plusieurs petits travaux simples.

Les classes peuvent être liées entre elles grâce au mécanisme d'héritage qui permet de mettre en évidence des relations de parenté. D'autres relations sont possibles entre des classes, chacune de ces relations est représentée par un arc spécifique dans le diagramme de classes.

Le diagramme suivant représente un diagramme de classes participantes du package Sécurité :

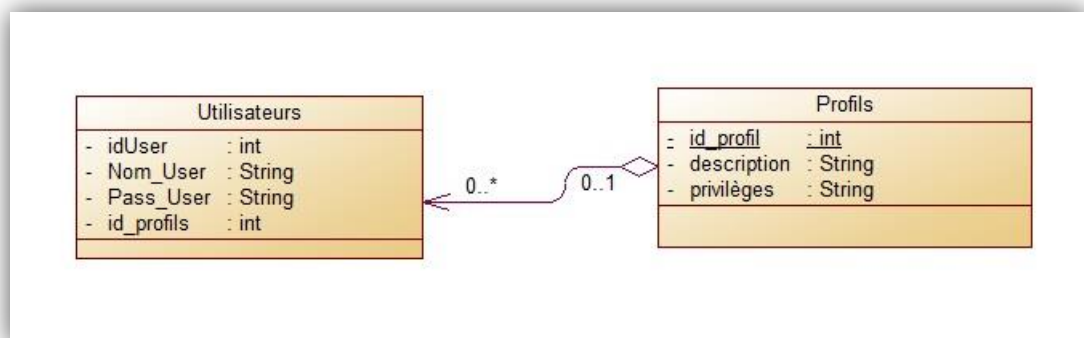


Figure 23 : Diagramme de classes participantes du package sécurité

Le diagramme suivant représente un diagramme de classes participantes du package Paramétrage :

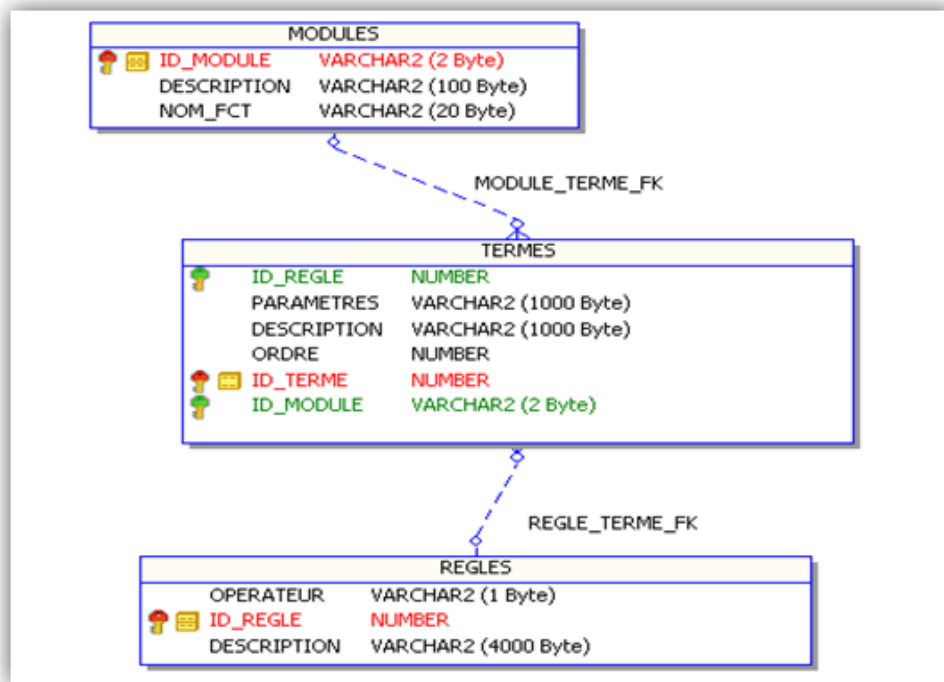


Figure 24 : Diagramme de classes participantes du package paramétrage

- ✓ **MODULES** : Classe regroupant chaque module, sa description et le nom de la fonction associée qui retourne une valeur.
- ✓ **REGLES** : Description des Règles.
- ✓ **TERMES** : paramétrage des termes de chaque règle et chaque module

3.2.4. Diagramme de séquence

Le diagramme de séquence est une description graphique des opérations d'un système sous un angle chronologique. C'est une vue dynamique qui contient les symboles d'objets (instances de classe), d'acteurs et de messages qu'ils échangent.

La dimension verticale est l'axe temporel : les messages y sont représentés par ordre chronologique. La dimension horizontale montre des objets et des acteurs qui échangent des informations.

Afin de mieux comprendre les séquences relatives au traitement nous présentons le diagramme de séquence suivant :

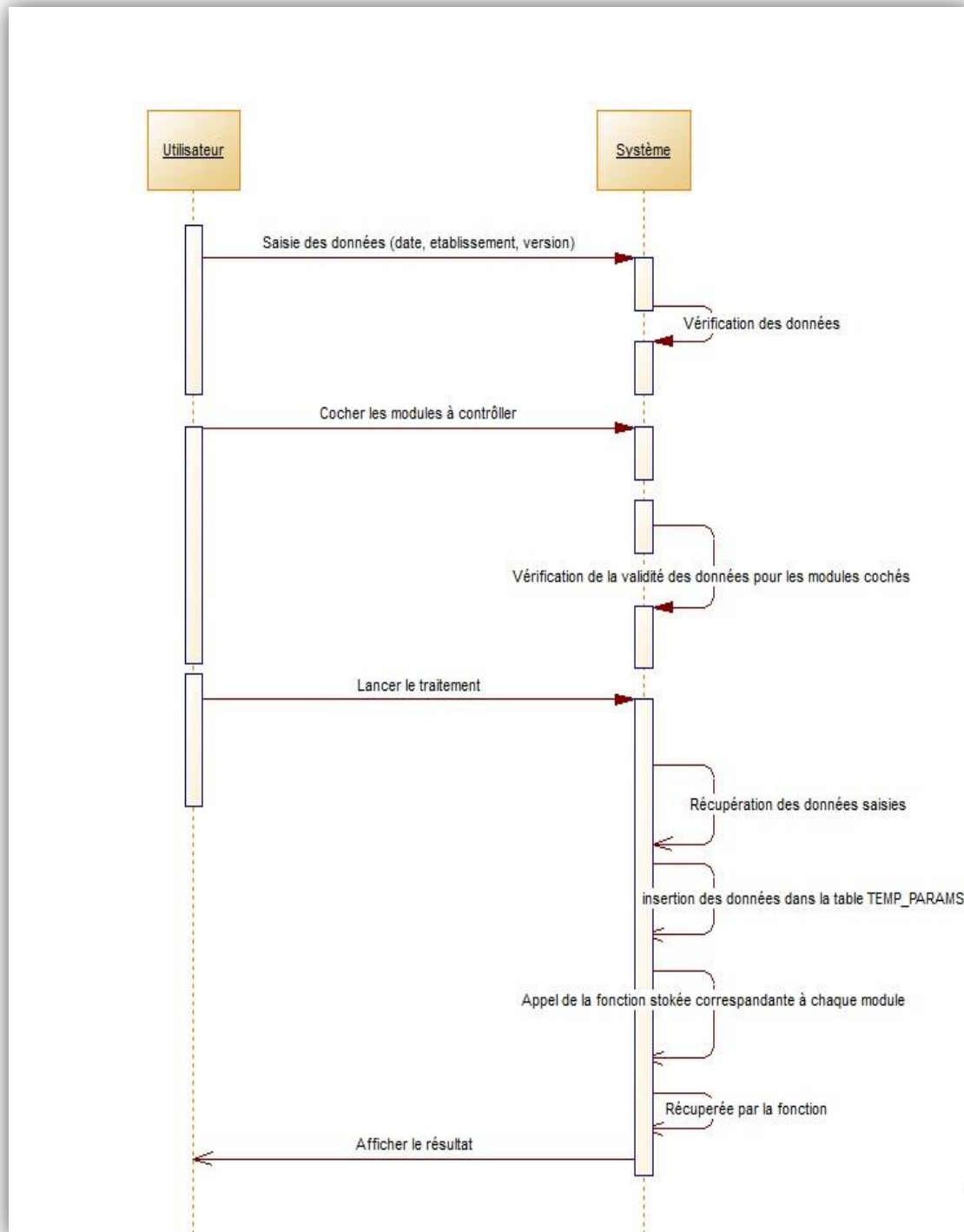


Figure 25 : Cas Diagramme de séquence du package traitement

Conclusion

Comme vu dans ce chapitre l'étape de l'analyse des risques est une étape critique qui influencera par la suite la bonne réalisation du projet, le respect du plan d'actions est une contrainte nécessaire pour la réussite de la nouvelle solution BRS MCM.

La conception est un procédé qui a pour objectif de permettre de formaliser les étapes préliminaires du développement d'un système afin de rendre ce développement plus fidèle aux besoins du client. Dans ce chapitre un ensemble de diagrammes UML ont été présentés afin d'illustrer la conception proposée pour la nouvelle solution.

Le chapitre suivant est réservé à la description de la réalisation de cette solution conformément à la conception proposée.

Chapitre 4**Mise en œuvre**

Dans ce chapitre nous allons présenter les différents outils utilisés pour la réalisation, ensuite nous allons détailler ce que nous avons réalisé pour résoudre les problèmes rencontrés dans l'application. Enfin nous allons présenter quelques interfaces de l'application.

4. Mise en œuvre

4.1. Outils utilisés

Dans cette partie nous présentons tout d'abord une description détaillée des outils utilisés dans notre plateforme et une explication de leurs principes de fonctionnement.

4.1.1. SGBD Oracle 11g

Oracle est un système de gestion de base de données relationnel (SGBDR) propriété fourni par Oracle Corporation leader mondial des bases de données et couramment utilisé dans les applications sur différentes plates-formes. Il a été développé par Lawrence Ellison, accompagné d'autres personnes telles que Bob Miner et Ed Oates [10].

➤ *Les fonctionnalités d'Oracle :*

Oracle est un SGBD permettant d'assurer :

- La définition et la manipulation des données
- La cohérence des données
- La confidentialité des données
- L'intégrité des données
- La sauvegarde et la restauration des données
- La gestion des accès concurrents

➤ *Les composants d'Oracle :*

Outre la base de données, la solution Oracle est un véritable environnement de travail constitué de nombreux logiciels permettant notamment une administration graphique d'Oracle, de s'interfacer avec des produits divers et d'assistants de création de bases de données et de configuration de celles-ci.

On peut classer les outils d'Oracle selon diverses catégories :

- Les outils d'administration
- Les outils de développement
- Les outils de communication
- Les outils de génie logiciel
- Les outils d'aide à la décision

➤ ***Outils de développement Oracle :***

Oracle propose également de nombreux outils de développement permettant d'automatiser la création d'applications s'interfaçant avec la base de données. Ces outils de développement sont :

- Oracle Designer
- Oracle Developer
- SQL*Plus : une interface interactive permettant d'envoyer des requêtes SQL et PL/SQL à la base de données
- Oracle Developer : il s'agit d'une suite de produits destinés à la conception et à la création d'applications client-serveur.

4.1.2. TOAD pour Oracle

TOAD pour Oracle est un environnement de développement puissant et léger conçu pour simplifier et accélérer le développement des bases de données et l'administration des applications au quotidien.

Destiné au spécialiste de bases de données, développeur PL/SQL, développeur d'application, administrateur ou analyste fonctionnel, TOAD pour Oracle répond à ses besoins et l'aide à atteindre un niveau supérieur de productivité.

TOAD réunit toutes les fonctions nécessaires pour la conception et l'exécution des requêtes, la création et la modification des objets de base de données, le développement et le débogage du code SQL ou PL/SQL. Même les tâches les plus courantes, telles que l'importation/exportation de données, la comparaison de schémas ou la mise à jour des statistiques, sont réalisées plus rapidement et plus facilement avec TOAD.

Il n'est pas nécessaire d'être un expert pour administrer de façon efficace les objets de base de données. L'explorateur de schéma TOAD Schéma Browser permet de visualiser rapidement le contenu de la base par une interface à onglet simple à utiliser.

TOAD affiche alors instantanément tous les détails de l'objet, éliminant l'exploration fastidieuse de longues listes de propriétés. Pour une plus grande simplicité d'utilisation,

tous les objets peuvent être également administrés à partir de la fenêtre de navigation principale.

4.1.3. Oracle Application Express

➤ *Présentation de l'outil Oracle Application Express*

Oracle Application Express, plus communément appelé Apex, est un environnement de développement permettant de créer des applications de type Web dont le but est d'accéder directement aux bases de données Oracle. A partir d'un simple navigateur Internet, les utilisateurs peuvent aller consulter les applications créées avec Apex et ainsi exploiter les données renseignées dans les bases de données.

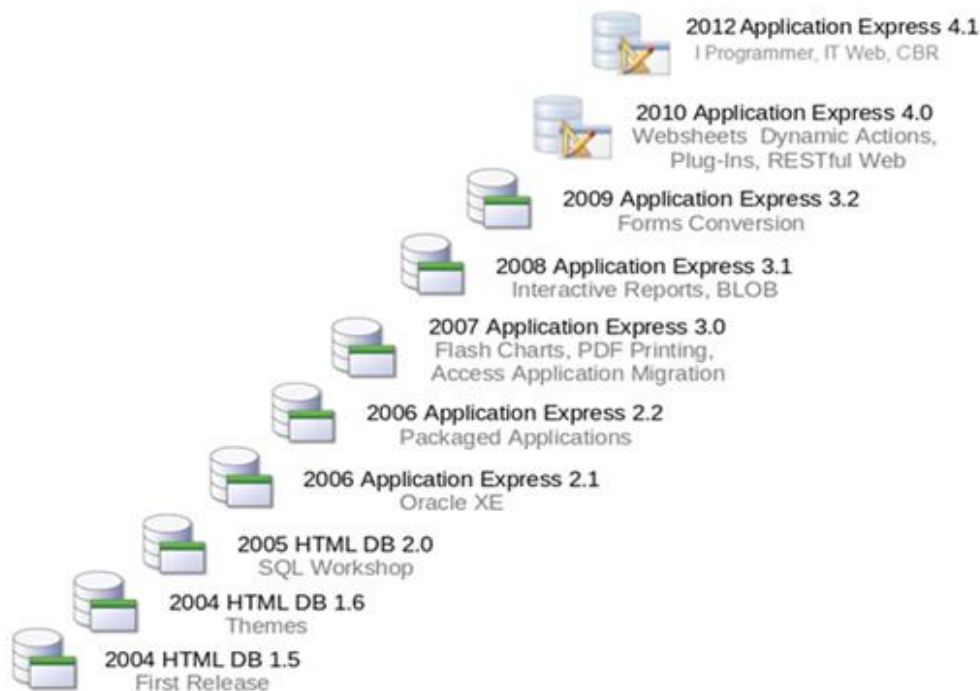


Figure 26 : Historique d'évolution d'APEX

➤ *Architecture 2 tiers d'APEX :*

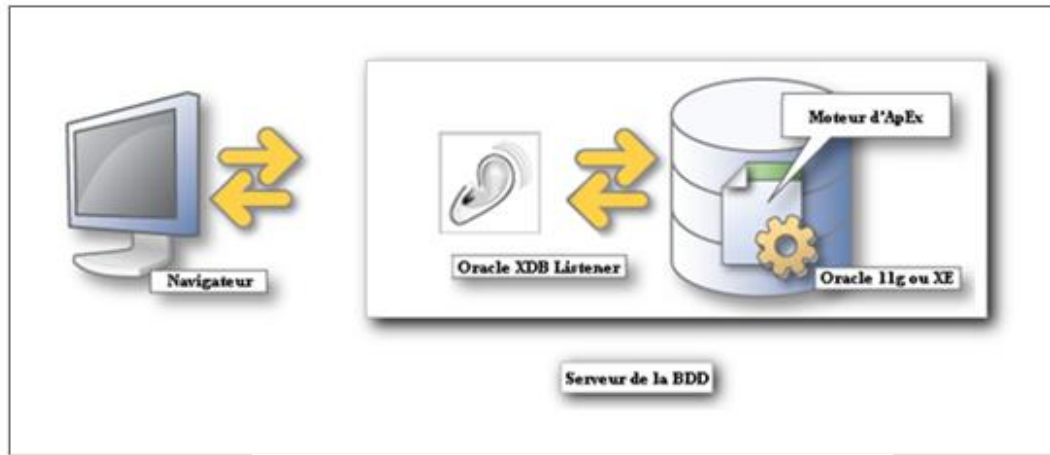


Figure 27 : Architecture 2-Tiers d'APEX

Les éléments de l'architecture 2-Tiers :

- Le navigateur Internet,
- Un serveur sur lequel se trouve:
 - La base de données contenant Apex,
 - Un listener HTTP se nommant Oracle XDB.

4.1.4. JavaScript

Le JavaScript est un langage informatique utilisé sur les pages web. Ce langage a la particularité de s'activer sur le poste client, en d'autres mots c'est votre ordinateur qui va recevoir le code et qui devra l'exécuter. C'est en opposition à d'autres langages qui sont activés côté serveur. L'exécution du code est effectuée par votre navigateur internet tel que Firefox ou Internet Explorer.

L'une des choses primordiales à savoir est de bien se rendre compte que le JavaScript n'a aucun rapport avec le Java qui est un autre langage informatique.

La particularité du JavaScript consiste à créer des petits scripts sur une page HTML dans

le but d'ajouter une petite animation ou un effet particulier sur la page. Cela permet en d'améliorer l'ergonomie ou l'interface utilisateur, mais certains scripts sont peu utile et servent surtout à ajouter un effet esthétique à la page. L'intérêt du JavaScript est d'exécuté un code sans avoir à recharger une nouvelle fois la page.

La technique AJAX (Asynchronous Javascript And XML) utilise grandement le JavaScript dans le but d'interagir sur la page de manière dynamique.

4.1.5. Langage PL/SQL

PL/SQL (sigle de Procedural Language / Structured Query Language) est un langage, conçu aux paradigmes procédural et structuré. Il est propriétaire, créé par Oracle et utilisé dans le cadre de bases de données relationnelles. Il a été influencé par le langage Ada.

PL/SQL est disponible dans Oracle Database (depuis la version 7), TimesTen In-Memory Database (depuis la version 11.2.1) et IBM DB2 (depuis la version 9.7).

Il permet de combiner des requêtes SQL et des instructions procédurales (boucles, conditions...), dans le but de créer des traitements complexes destinés à être stockés sur le serveur de base de données (objets serveur), comme des procédures stockées ou des déclencheurs.

Les dernières évolutions proposées par Oracle reposent sur un moteur permettant de créer et gérer des objets contenant des méthodes et des propriétés.

À la base, PL/SQL est un langage interprété, mais depuis la version 9i RC1, le code peut être compilé en code machine. Dans la version 9i d'Oracle database, le code est converti en C puis doit être compilé en librairies partagées (DLL sous Windows), dans la version 10g le code machine est stocké dans le catalogue et depuis la version 11g il est stocké dans le tablespace système après compilation directe.

D'autre part le langage PL/SQL permet de faire appel à des procédures externes, c'est-à-dire des procédures écrites dans un autre langage (de troisième génération, généralement le langage C).

4.2. Cryptage des données et échange de clés

4.2.1 . Le package DBMS_CRYPTO

DBMS_CRYPTO est un package qui existe depuis la version Oracle 10g et qui permet l'encryptions des données. Anciennement nommé **DBMS_OBFUSCATION_TOOLKIT**, ce nouveau package possède des algorithmes de **cryptage** et des fonctions de **chiffrement** plus puissants.

Nous avons utilisés l'algorithme de cryptage AES128 (Advanced Encryptions Standard 128 bits), une fonction de cryptage, une fonction de décryptage et une fonction de padding.

Pour des raisons de sécurité, nous avons choisi de mettre la clé en dehors de la base de données car les données cryptées dans un export Full ou User seront illisibles car la clé n'est pas exportée avec la base et la fonction de **décryptage** ou **cryptage** plantera simplement si les données sont chargées sur un autre environnement.

4.2.2. Le protocole SSL

SSL (**Secure Sockets Layers**, que l'on pourrait traduire par ***couche de sockets sécurisée***) est un procédé de sécurisation des transactions effectuées via Internet. Le standard SSL a été mis au point par *Netscape*, en collaboration avec *Mastercard*, *Bank of America*, *MCI* et *Silicon Graphics*. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet. Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification [11].

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport .De cette manière, SSL est transparent pour l'utilisateur (entendez par là qu'il peut ignorer qu'il utilise SSL). Par exemple un utilisateur utilisant un navigateur internet pour se connecter à un site de commerce électronique sécurisé par SSL enverra des données chiffrées sans aucune manipulation nécessaire de sa part

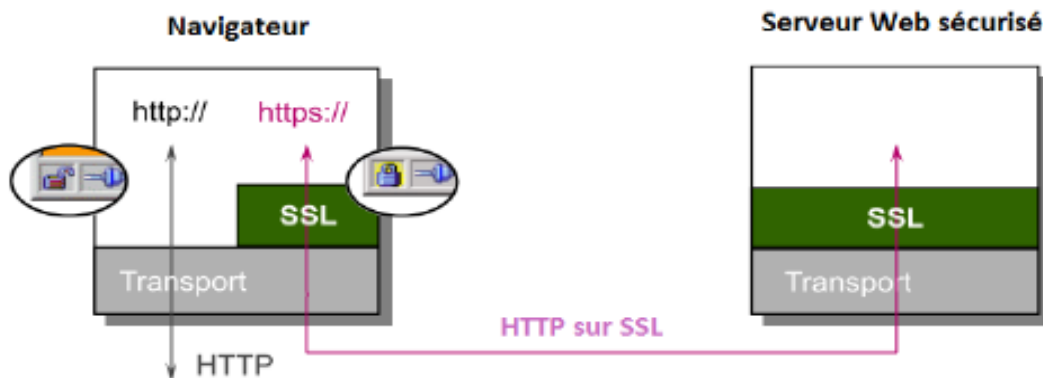


Figure 28 : Utilisation de SSL par le protocole HTTP

4.3 . La mise en œuvre

En ingénierie et plus particulièrement en informatique, la mise en œuvre désigne la création d'un produit fini à partir d'un document de conception, d'un document de spécification, voire directement depuis une version originelle ou d'un cahier des charges. Cette partie décrit les étapes de mise en œuvre de la solution ainsi que son déploiement chez le client.

4.3.1 . Les étapes de la mise en œuvre

Après avoir développé l'application sous la plate-forme Oracle Apex on s'est retrouvé devant l'obligation de tester le déploiement de l'application chez le client, on a pris comme client de teste la société d'accueil elle-même : OMNIDATA.

- La première étape consistait à mettre en place une machine virtuelle sur laquelle s'installera l'application Inter Déclaration
- La seconde étape consistait à installer Oracle 11g sur la machine (Annexe C)
- La troisième étape c'est la création du schéma de la base de données Change.
- La quatrième étape c'est l'intégration de APEX 4.1 dans Oracle 11g
- La cinquième étape consistait à implémenter la solution retenue.
- Finalement procéder à la phase de test.

4.3.2 . Résultat de la mise en œuvre

Après avoir terminé toutes ces étapes, le résultat s'est avéré positif, l'application fonctionne correctement et respecte ce qui a été décrit sur le cahier des charges.

Les figures suivantes présentent la partie de concrétisation du projet en illustrant les prises d'écran de l'application réalisée.

➤ ***Ecran authentication :***

Ce premier écran permet de saisir le nom de l'utilisateur et le mot de passe correspondant. Les utilisateurs et leurs droits d'accès sont définis par l'Administrateur de la solution BRSMCM

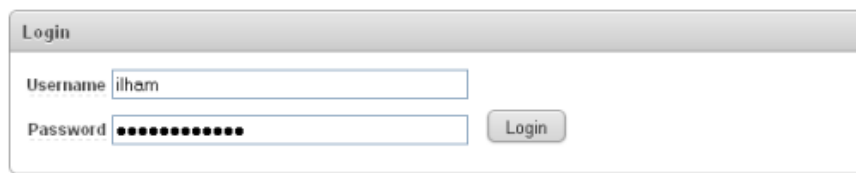


Figure 29 : Ecran d'authentification

➤ ***BRS MCM : Menu général :***

Toutes les transactions élémentaires de BRSMCM fonctionnent suivant le mode de fonctionnement standard Oracle APEX et apparaissent avec une barre d'outils pour répondre aux différents besoins de recherche, insertion, modification...

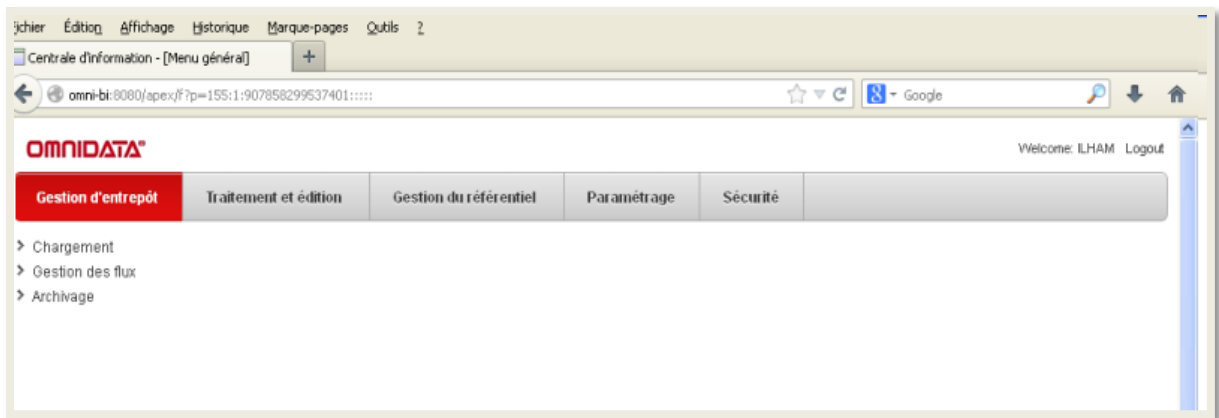


Figure 30 : Menu général de BRS MCM

➤ **Gestion d'entrepôt ➤ Chargement :**

Cette transaction permet de charger, par domaine, les flux sources conformément à l'entrée standard de BRSMCM dans l'entrepôt dédié au marché des changes et monétaire.

Type Compartiment
Position change
Change Terme
Swap de devise
Options de change
Prets et emprunts en devises
Encours global du portefeuille des options de change
Achats et ventes de titre ou instrument financier à l'étranger
Change sur les produits de base

Figure 31 : Ecran chargement des données à partir des fichiers sources

➤ ***Gestion d'entrepôt → Chargement → Marché des changes → Position de change :***

Cette transaction permet de consulter et gérer les données « Position de change » chargées sur l'entrepôt de BRSMCM.

Date position	Devise	Avoir bilan	Engagement bilan	Avoir spot hors bilan	Avoir terme hors bilan	Engagement spot hors bilan	Engagement terme hors bilan	Couverture position optionnelle
20/03/2012		10000	200000	30000	40000	50000	60000	7000
20/03/2012	USD	0	0	30000		50000	60000	7000
20/03/2012	USD	55	0	30000	40000	50000	60000	7000
20/03/2012	USD	0	0	30000		50000	60000	7000
20/03/2012		7777	200000	30000	40000	50000	60000	7000
20/03/2012	USD	0	200000	30000	40000	50000	60000	7000
20/03/2012	USD	55	0	30000	40000	50000	60000	7000
20/03/2012	USD	0	0	30000		50000	60000	7000

Figure 32 : Consultation des données « position de change »

➤ ***Traitement et édition → Contrôle :***

Il s'agit d'une phase primordiale du processus de déclaration, dans le sens où l'utilisateur procède aux contrôles exhaustifs des données à déclarer avant de générer les fichiers XML. Cette fonctionnalité lui permettra de simuler, par domaine, le retour BAM via l'édition d'un rapport des anomalies éventuelles relevées sur la déclaration

Figure 33 : Contrôle des données à déclarer

- Vérifier que les paramètres d'entrée (Date, Version, établissement) sont bien positionnés
- Sélectionner le domaine de déclaration souhaité (Marché des Changes ou Marché Monétaire)
- Sélectionner le type de compartiment à contrôler
- Appuyer sur le bouton « Lancer Contrôle »
- Un message notifiant la fin de la transaction s'affiche à l'écran.
- Pour visualiser le contenu du rapport de contrôle, appuyer sur « Afficher Log ».

Un document similaire au rapport ci-après s'affiche :

Figure 34 : Document rapport de contrôle des fichiers d'échange

➤ **Traitement et édition** → **Génération fichier XML :**

Une fois les contrôles sont appliqués et les anomalies relatives aux données sont rectifiées, l'utilisateur peut procéder à la génération, par domaine, d'un ou de la totalité des fichiers XML à destination de BAM.

The screenshot shows a web application interface for generating XML files. At the top, there is a navigation bar with tabs: 'Gestion d'entrepôt', 'Traitement et édition' (highlighted in red), 'Gestion du référentiel', 'Paramétrage', and 'Sécurité'. Below the navigation bar, there is a sub-header 'Génération fichier(s) Xml'. The main area is divided into two sections: 'Paramétrage' and 'Domaine'. The 'Paramétrage' section contains three input fields: 'Date déclaration', 'Etablissement', and 'Version'. The 'Domaine' section contains a dropdown menu with the selected value '02: Marché monétaire'. Below the dropdown menu, there is a table with the following content:

Type Compartiment
Prêts et emprunts en blanc
Opérations de Pensions livrées
Opérations fermes du marché secondaire des BOT
TCN Marche Primaire
TCN Marche Secondaire
Encours TCN
Depôts à Terme

At the bottom of the form, there is a button labeled 'Génération fichier Xml'.

Figure 35 : Ecran de génération des fichiers XML

- Vérifier que les paramètres d'entrée (Date, Version, établissement) sont bien positionnés
- Sélectionner le domaine de déclaration souhaité (Marché des Changes ou Marché Monétaire)
- Sélectionner le type de compartiment pour lequel l'utilisateur souhaite générer le fichier XML
- Appuyer sur le bouton « Générer fichiers XML »
- Un message notifiant la fin de la transaction s'affiche à l'écran.
- Visualiser le résultat de la génération des fichiers XML sélectionnés au niveau du chemin indiqué sur le message qui s'affiche.

➤ **Sécurité → Gestion des profils :**

Cette transaction permet de créer les profils et de gérer les accès aux modules de BRSMCM. Chaque utilisateur sera affecté à un profil donné qui définira son accès à l'application.

Les profils pré-paramétrés dans la solution BRSMCM sont :

- **Administrateur** : ce profil permet l'accès uniquement au module d'administration (sécurité)
- **Exploitant** : ce profil permet de faire tous les traitements au niveau de BRSMCM mais ne donne pas accès au référentiel sauf en mode « Consultation »
- **Administrateur Fonctionnel** : Ce profil donne accès juste au Référentiel de BRSMCM.

La création d'un profil est effectuée à partir du menu : « Sécurité > Gestion des profils ». L'administrateur renseigne les éléments suivants :

- **Nom** : un nom significatif du profil
- **Description** : description du profil
- **Code module** : l'administrateur sélectionne le code module auquel le profil aura accès.
- **Description module**
- **Droit d'accès** :
 - C : « Création » lorsque cette case est cochée, l'utilisateur a le droit de créer un nouvel enregistrement sur ce module
 - M : « Modification » lorsque cette case est cochée, l'utilisateur a le droit de modifier un enregistrement sur ce module
 - S : « Suppression » lorsque cette case est cochée, l'utilisateur a le droit de supprimer un enregistrement sur ce module

- I : « Interrogation » lorsque cette case est cochée, l'utilisateur a le droit de consulter un ou plusieurs enregistrements d'un module

<input type="checkbox"/>	Code	Description	C	M	S	I
<input type="checkbox"/>	801	Chargement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	802	Position de change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	803	Change spot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	804	Change terme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	805	Swap de devise	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 36 : Gestion des profils

➤ **Sécurité** ➔ **Gestion des utilisateurs :**

Cette transaction permet de saisir les utilisateurs de BRSMCM et de leur affecter un profil.

Figure 37 : Gestion des utilisateurs

L'administrateur crée l'utilisateur, lui affecte un mot de passe et un profil.

L'utilisateur peut par la suite changer son mot de passe à partir du menu « Paramétrage > Options > Sécurité » dans BRSMCM.

Conclusion

Ce chapitre a permis de faire la description du travail réalisé dans le cadre de mon projet de fin d'études, notamment en présentant d'abord les outils et protocoles utilisés, et en illustrant par la suite par des captures d'écrans l'application réalisée ainsi que de la partie sécurité pour la gestion des profils et des utilisateurs ont été .

Conclusion générale

La génération des fichiers XML et le contrôle des flux transmis à BAM pour les marchés des changes et monétaire se fait à l'aide d'un système intitulé BRS MCM (Bank Reporting System pour les marchés des changes et monétaire)

Cette solution était réalisée par Oracle Forms 6i, elle connaissait grand nombre de faiblesses, notre projet de fin d'études consistait à remplacer le système existant par une autre solution plus performante : BRS MSM sous Oracle Apex , la mise en place du protocole SSL pour sécuriser le transfert des flux et la gestion des droits d'accès aux différents modules de la solution.

La refonte du système déjà instauré est passée par plusieurs étapes cruciales, notamment : dégager les faiblesses du système existant, analyser les impacts fonctionnels et techniques pour avoir une vision claire sur le travail réalisé et sur la démarche à suivre, faire l'analyse des risques , établir un plan d'actions à suivre pour minimiser les risques et refaire la conception , développer la nouvelle solution qui est une application web avec un nouvel outil innovant qui est Oracle APEX. Nous avons suivi pour mener à bien le projet une méthodologie rigoureuse de travail, se basant sur la méthode de développement en cascade), ensuite nous avons réalisé des tests de l'application et enfin nous l'avons déployé. Aussi, parmi les tâches réalisées nous citons la gestion des profils et utilisateurs en assurant la granularité des accès aux bases de données et en évitant d'affecter aux utilisateurs des rôles conflictuels , l'implémentation des procédures de cryptage basées sur des algorithmes robustes (AES 128), et l'utilisation du protocole SSL pour sécuriser les échanges de fichiers entre les banques, les établissements de crédit et BAM.

Par ailleurs, ce projet nous a permis de mettre en pratique notre esprit d'étude, d'analyse et de synthèse. De mettre en application certaines de nos connaissances et notre savoir acquis lors de la période de la formation à l'ENSIAS et de découvrir la différence entre les projets professionnels et ceux à caractère pédagogique.

Références bibliographiques

Bibliographie :

[11] Hanane El BAKKALI, *Cours de la sécurité applicative 3A*, version 19, janvier 2013

[1] *Déclaration à la centrale d'informations BAM pour les marchés des changes et monétaire*, Manuel d'utilisation Version 1.4, Casablanca ,12 Avril 2012.

Webographie :

[2] Alazard CAMUS, *Modèle en cascade*, Mai 2008, [En ligne] Date de dernière mise à jour : Août 2010. Disponible sur :

http://www.umc.edu.dz/vf/coursLigne/MSI/Modele_developpement_logiciel.html

[6] Jean-Philippe JOUAS, *Guide de diagnostic de l'état des services de sécurité*, Août 2000, [En ligne] Date de dernière mise à jour : le Août 2010.

Disponible sur : <http://www.transferts-lr.org/content/.../fr-doc-mehari-2000.pdf>, 12 avril 2011

[7] Jean-Philippe JOUAS, *Guide de l'analyse des enjeux et de la spécification*, Août 2000, [En ligne] Date de dernière mise à jour : le Août 2010.

Disponible sur : <http://www.transferts-lr.org/content/.../fr-doc-mehari-2000.pdf>, 12 avril 2011

[8] Jean-Philippe JOUAS, *Manuel de référence de service de sécurité*, Août 2000, [En ligne] Date de dernière mise à jour : le Août 2010.

Disponible sur : <http://www.transferts-lr.org/content/.../fr-doc-mehari-2000.pdf>, 12 avril 2011

[4] Jean-Philippe JOUAS, *Methodes de MEHARI*, Août 2000, [En ligne] Date de dernière mise à jour : le Août 2010.

Disponible sur : <http://www.transferts-lr.org/content/.../fr-doc-mehari-2000.pdf>, 12 avril 2011

[3] Luigi GIURI , *Role templates for content-based access control* , Published in New York, NY, USA , [En ligne] Date de dernière mise à jour : 2011 , nombre de pages : 153-159.

Disponible sur : <http://dl.acm.org/citation.cfm?id=266773>

[10] Eugene PARK , *Lowering Your IT Costs with Oracle Database 11 g Release 2* , Février 2011 ,nombre de pages 122.

Disponible sur :

<http://www.oracle.com/us/products/database/039448.pdf?ssSourceSiteId=ocomfr>

[9] Pascal ROQUES, *UML 2 par la pratique*, Edition EYROLLES, 2008, nombres de pages 387.

Annexes

Annexe A : Tableau d'impact intrinsèque

Annexe B : Tableau des vulnérabilités intrinsèques

Annexe C : Manuel d'installation d'Oracle APEX

Annexe A

Tableau d'impact intrinsèque

Tableau d'Impact Intrinsèque				Sélection d'actifs
Actifs de type Données et informations				
	D	I	C	
Données et informations				
D01 Fichiers de données ou bases de données applicatives	4	3	3	1
D02 Fichiers bureautiques partagés	3	3	1	1
D03 Fichiers bureautiques personnels (gérés dans environnement personnel)				1
D04 Informations écrites ou imprimées détenues par les utilisateurs, archives personnelles				1
D05 Listings ou états imprimés des applications informatiques			2	1
D06 Données échangées, écrans applicatifs, données individuellement sensibles	3	2	1	1
D07 Courrier électronique		2		1
D08 Courrier postal et télécopies		2		1
D09 Archives patrimoniales ou documentaires				1
D10 Archives informatiques	2	1	1	1
D11 Données et informations publiées sur des sites publics ou internes	3	3	2	1
Actifs de type Services				
	D	I	C	
Services généraux communs				
G01 Environnement de travail des utilisateurs				1
G02 Services de télécommunication (voix, télécopies, visioconférence, etc.)	1	1		1
Services informatiques et réseaux				
R01 Service du réseau étendu	3	2		1
R02 Service du réseau local	3	3		1
S01 Services applicatifs	3	2	2	1
S02 Services bureautiques communs (serveurs de données, gestionnaires de documents, imprimantes partagées, etc.)				1
S03 Equipements mis à la disposition des utilisateurs (PC, imprimantes locales, périphériques, interfaces spécifiques, etc.)	2			1
Nota : Considérer ici la perte massive de ces services et non celle d'un seul utilisateur				
S04 Services systèmes communs : messagerie, archivage, impression, édition, etc.				1
S05 Services de publication d'informations sur un site web interne ou public	2	3		1
Actifs de type Processus de gestion				E
Processus de gestion de la conformité à la loi ou à la réglementation				
C01 Conformité à la loi ou aux réglementations relatives à la protection des renseignements personnels				1
C02 Conformité à la loi ou aux réglementations relatives à la communication financière				1
C03 Conformité à la loi ou aux réglementations relatives à la vérification de la comptabilité informatisée	3			1
C04 Conformité à la loi ou aux réglementations relatives à la propriété intellectuelle	3			1
C05 Conformité à la loi relative à la protection des systèmes informatisés	3			1
C06 Conformité aux réglementations relatives à la sécurité des personnes et à la protection de l'environnement	3			1
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.				
Il faut mettre 0 dans la colonne F (sélection d'actifs) pour dé-sélectionner l'actif correspondant.				
Attention : Cette facilité équivaut à donner un impact nul pour tous les scénarios attachés à cet actif.				
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.			

Tableau d'impact intrinsèque (MEHARI 2010)

Annexe B

Tableau des vulnérabilités

intrinsèques

Tableau des vulnérabilités intrinsèques					
Type d'actif secondaire	Type de dommage subi	Type de vulnérabilité	Critère	Code	Sélection
Catégorie : Service					
Configuration logicielle	Altération	Possibilité d'altération des configurations logicielles (logiciels et paramètres)	D et I	Cfl.alt	1
	Non fonctionnement	Possibilité de non fonctionnement intrinsèque d'un logiciel (bug)	D	Cfl.bug	1
	Divulgarion de logiciel	Possibilité de diffusion de fichier de logiciel	C	Cfl.dif	1
	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	1
	Pollution	Possibilité de pollution des configurations logicielles	I	Cfl.pol	1
Compte ou moyen d'accès au service	Blocage	Possibilité de blocage des comptes utilisateurs	D	Cpt.blo	1
	Disparition	Possibilité de perte des moyens nécessaires à la connexion au service	D	Cpt.dis	1
Équipement 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	1
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	Possibilité d'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	1
Catégorie : données					
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	1
Données en transit, messages, écrans	Altération	Possibilité d'altération de données en transit ou messages	I	Dtr.alt	1
	Divulgarion	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
	Divulgarion	Possibilité de duplication ou diffusion (et divulgation) de fichier support de données	C	Fic.dif	1
	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	1
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	1
	Echange	Possibilité d'échange de media support de données	D et C	Med.ech	1
	Inexploitabilité	Possibilité d'inexploitabilité de media support de données	D	Med.ine	1
Catégorie : processus de management					
Procédures et directives	Inefficacité	Possibilité que les procédures appliquées soient inefficaces (vis-à-vis des obligations légales, réglementaires ou contractuelles)	E	Pro.inf	1

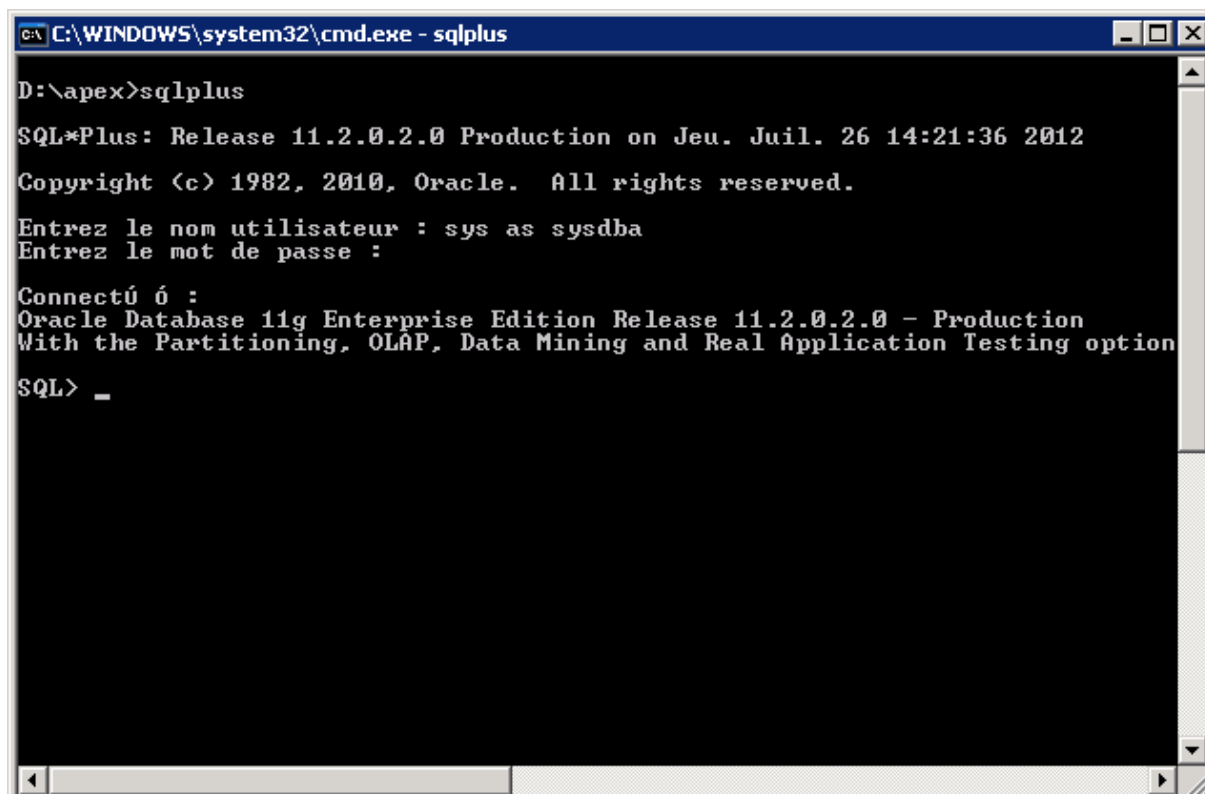
Tableau des vulnérabilités intrinsèques

Annexe C

**Manuel d'installation d'Oracle
APEX**

Installation d'APEX 4.1

1. Décompresser le fichier « apex_4.1.1.zip » dans un répertoire tel que « D:\ »
2. Ouvrir l'invite de commande DOS.
3. Déplacez-vous dans le répertoire créé: « D:\apex »
4. Connectez-vous en tant que SYSDBA dans votre SQLPlus:



```
C:\WINDOWS\system32\cmd.exe - sqlplus

D:\apex>sqlplus

SQL*Plus: Release 11.2.0.2.0 Production on Jeu. Juil. 26 14:21:36 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.

Entrez le nom utilisateur : sys as sysdba
Entrez le mot de passe :

Connecté à :
Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing option
SQL> _
```

5. Lancer la commande : @apexins SYSAUX SYSAUX TEMP /i/
6. Lancer la commande : @apxldimg.sql APEX_HOME _INSTALL

Où APEX_HOME_INSTALL est le répertoire qui contient votre répertoire apex.
C'est-à-dire c'est là où vous avez mis votre archive apex_4.1.1.zip et non le répertoire qu'il vous a créé lors de la décompression de l'archive.

- Dans notre cas c'est : « D:\ »
- La commande devient : @apxldimg.sql D:\

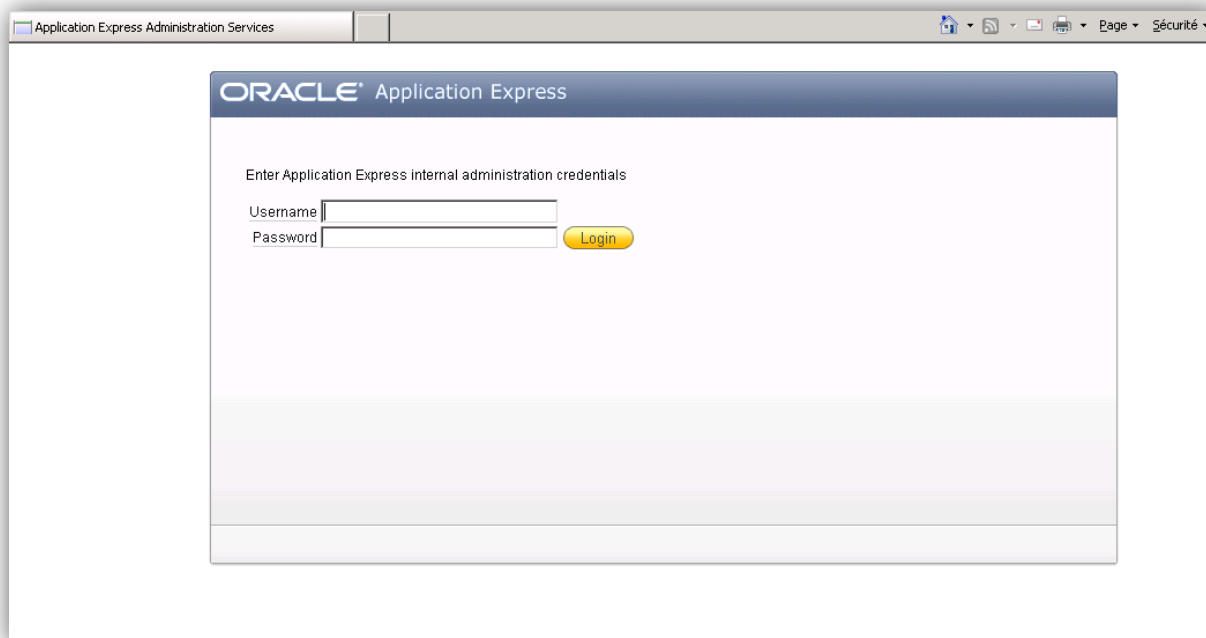
7. Se reconnecter en tant que SYSDBA.
8. Lancer la commande : @apxconf
 - Entrer le mot de passe ADMIN.
 - Entrez le port sur lequel vous voulez que le serveur web tourne. (8080 par défaut).
9. Lancer la commande :
 - ALTER USER anonymous ACCOUNT UNLOCK
10. Déconnectez-vous

Configuration du Workspace :

Maintenant que tout est bien installé et prêt, il est temps de vous connecter à l'administration d'APEX. Pour ceci, ouvrez un navigateur web et allez à l'adresse : http://server-ip:port-choisit/apex/apex_admin

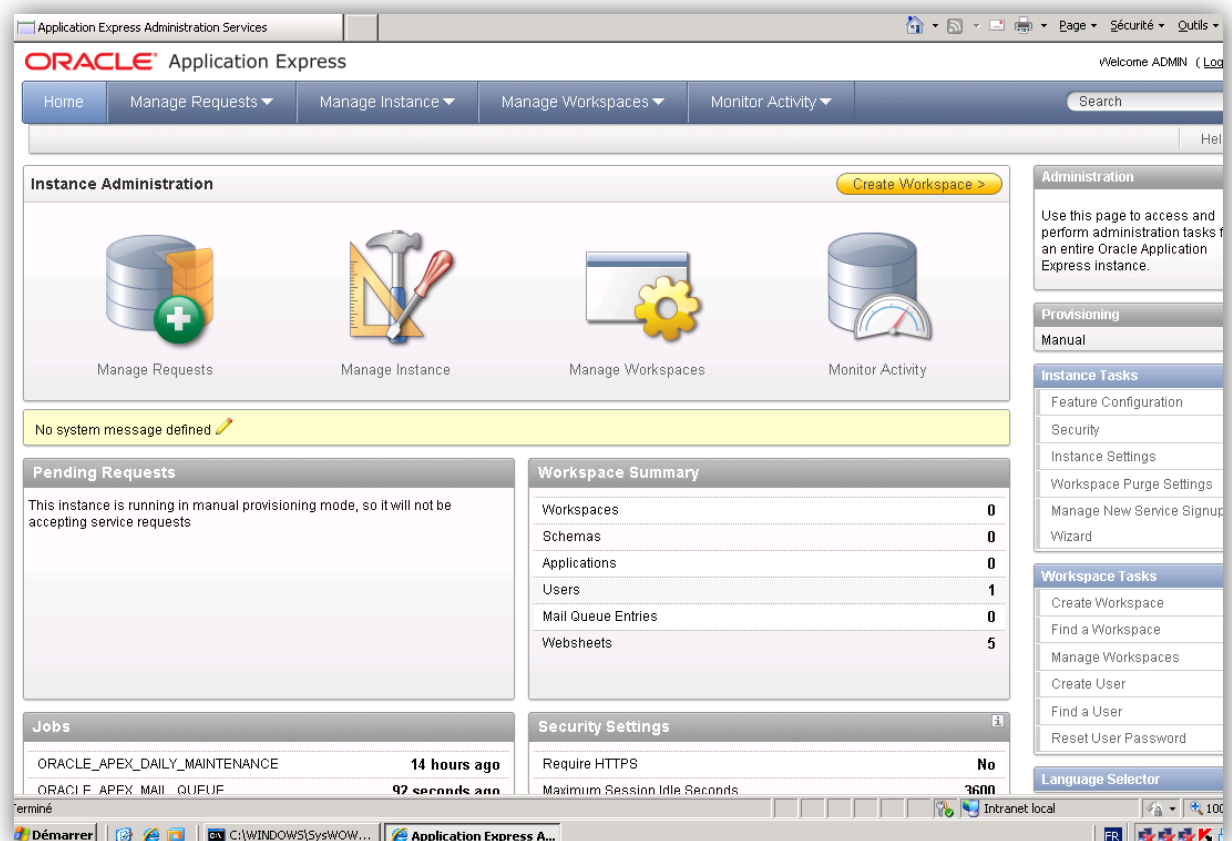
- Dans notre cas : http://localhost:8080/apex/apex_admin

Cette page apparaît :



Ecran de login de l'administration APEX

Rentrez le login *ADMIN* et votre mot de passe défini lors de l'installation. Vous arrivez sur cette page :



Ecran d'administration APEX

- Cliquez sur la flèche à côté de l'icône *Manage Workspaces* => *Manage Workspaces* => *Create Workspaces*.

Vous arrivez sur cet écran :

The screenshot shows the Oracle Application Express interface. The top navigation bar includes 'Home', 'Manage Requests', 'Manage Instance', 'Manage Workspaces', and 'Monitor Activity'. The breadcrumb trail is 'Home > Manage Workspaces > Create Workspace'. On the left, a vertical list of steps is shown: 'Identify Workspace' (highlighted in yellow), 'Identify Schema', 'Identify Administrator', 'Confirm Request', and 'Success Confirmation'. The main panel is titled 'Create Workspace' and contains three input fields: 'Workspace Name' (with a red asterisk), 'Workspace ID', and 'Workspace Description' (a text area). 'Cancel' and 'Next >' buttons are in the top right corner.

Créer Workspace - Etape 1

- Donnez un nom à votre Workspace et un commentaire.
- Vous cliquez sur **Next >**

The screenshot shows the 'Create Workspace' screen at Step 2. The left sidebar now highlights 'Identify Schema'. The main panel has a title bar with 'Cancel', '< Previous', and 'Next >' buttons. Below the title bar, there is instructional text: 'Select whether or not the schema already exists. If the schema exists, select the schema from the list. If the schema does not exist, enter a name and password and choose the size of the associated tablespace to be created.' The form includes a dropdown for 'Re-use existing schema?' set to 'No', a 'Schema Name' field with the value 'CHANGE', a 'Schema Password' field with masked characters, and a 'Space Quota (MB)' dropdown set to '10'.

Créer Workspace - Etape 2

- Oracle vous demande le schéma auquel est rattaché le Workspace.
- Vous avez le choix entre utiliser un schéma existant ou en créer un nouveau.
- Vous cliquez sur **Next** ➤

The screenshot shows the 'Create Workspace' wizard in Oracle Application Express. The left sidebar contains a sequence of steps: Identify Workspace, Identify Schema, Identify Administrator (highlighted in yellow), Confirm Request, and Success Confirmation. The main panel is titled 'Create Workspace' and contains the following fields:

- Administrator Username: ADMIN
- Administrator Password: (masked with dots)
- First Name: admin
- Last Name: admin
- Email: admin@omnidata.ma

Navigation buttons at the top right include 'Cancel', '< Previous', and 'Next >'.

Créer Workspace - Etape 3

Donner l'identité de l'utilisateur qui pourra administrer complètement ce Workspace. Cet utilisateur est complètement indépendant d'un utilisateur Oracle ou de votre utilisateur *Admin* précédemment créé. vous cliquez sur Next ➤

The screenshot shows the 'Confirm Request' step of the 'Create Workspace' wizard. The left sidebar highlights the 'Confirm Request' step. The main panel displays a confirmation message and the following information:

- Workspace Information:**
 - Name: XBM
 - Security Group ID: System Assigned
 - Description: XBRL, BRS, MCM...
- Administrator Information:**
 - User Name: ADMIN
 - E-mail: admin@omnidata.ma
- Schema Information:**
 - Reuse Existing Schema: Yes
 - Schema Name: CHANGE

Navigation buttons at the top right include 'Cancel', '< Previous', and 'Create Workspace'.

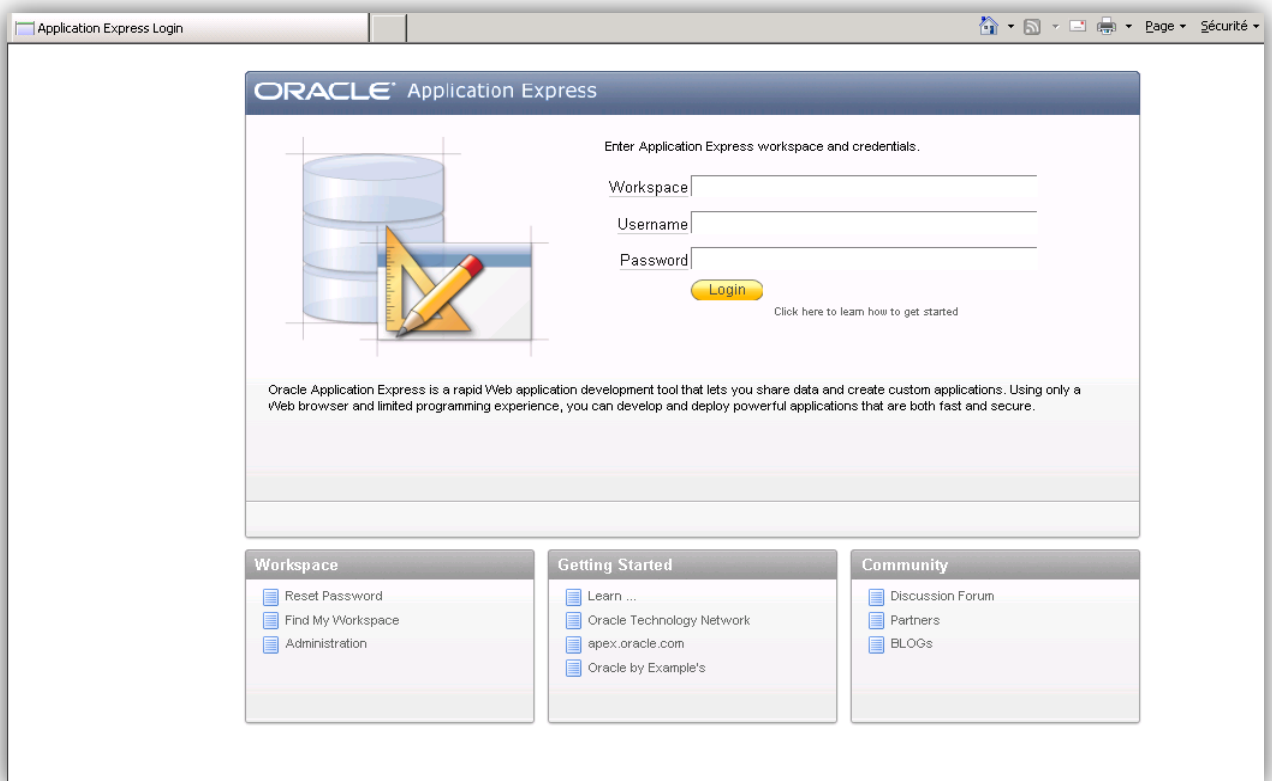
Créer Workspace - Etape 4

- Oracle vous donne un résumé de ce que vous allez créer.
- Cliquez sur *Create Workspace* et votre Workspace sera créée.

Accéder au Workspace

- Taper l'adresse suivante : `http://server-ip:port-choisit/apex`
- Dans notre cas : `http://localhost:8080/apex`

Vous arrivez sur cette page :



Ecran Login de votre Workspace

- Entrer le nom de votre Workspace, votre login et votre mot de passe créé dans la partie précédente.

Vous arrivez sur cette page :

Workspace crée précédemment

