



École Supérieure Africaine des Technologies de
l'Information et de la Communication



NEXORA

MÉMOIRE DE FIN DE CYCLE POUR L'OBTENTION DU MASTER

EN SYSTÈMES D'INFORMATION ET GÉNIE LOGICIEL (SIGL)

CONCEPTION D'UNE PLATEFORME NUMERIQUE D'EVALUATION DU
RISQUE DE CONFORMITE REGLEMENTAIRE : CAS DE LA LUTTE
CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU
TERRORISME

M-26.SAV.513

Période de stage : Du 05 janvier au 03 juillet 2026
Présenté par :

SAVANE Mouhamed

Encadrant Académique :

Dr COULIBALY Kpinna Tiekoura

Maitre de conférence

Dr GOLI CHARLES ETIENNE

Enseignant-chercheur

Maître de stage :

M GILLES YAO

Responsable Technique de Développement Digital

JURY

Président : Prof. SORO Etienne, Enseignant-chercheur à l'ESATIC

Rapporteur : Dr. KOFFI Dagou Dangui Augustin, Enseignant-chercheur à l'ESATIC

Assesseur : M. KPON Roger, Chef de service technologie et SI au CSRS

Membre : Dr. SILUE Nonfara Aliatou, Enseignante-chercheuse à l'ESATIC



École Supérieure Africaine des Technologies de
l'Information et de la Communication



NEXORA

MÉMOIRE DE FIN DE CYCLE POUR L'OBTENTION DU MASTER

EN SYSTÈMES D'INFORMATION ET

GÉNIE LOGICIEL (SIGL)

CONCEPTION D'UNE PLATEFORME NUMERIQUE D'EVALUATION DU
RISQUE DE CONFORMITE REGLEMENTAIRE : CAS DE LA LUTTE
CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU
TERRORISME

M-26.SAV.513

Période de stage : Du 05 janvier au 03 juillet 2026
Présenté par :

SAVANE Mouhamed

Encadrant Académique :

Dr COULIBALY Kpinna Tiekoura

Maitre de conférence

Dr GOLI CHARLES ETIENNE

Enseignant-chercheur

Maître de stage :

M GILLES YAO

Responsable Technique de Développement Digital

JURY

Président : Prof. SORO Etienne, Enseignant-chercheur à l'ESATIC

Rapporteur : Dr. KOFFI Dagou Dangui Augustin, Enseignant-chercheur à l'ESATIC

Assesseur : M. KPON Roger, Chef de service technologie et SI au CSRS

Membre : Dr. SILUE Nonfara Aliatou, Enseignante-chercheure à l'ESATIC

RÉSUMÉ

Ce mémoire présente la conception et le développement d'une plateforme numérique centralisée d'évaluation du risque de conformité en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). En s'appuyant sur une méthodologie rigoureuse pour analyser les besoins des acteurs de la conformité réglementaire, il décrit comment l'association de technologies modernes telles que les architectures SaaS multi-tenant, l'automatisation des processus métier, l'analyse des risques et la gestion centralisée des données permet de répondre aux exigences réglementaires du secteur.

Cette étude met en évidence l'apport des systèmes d'information dans l'amélioration de la gouvernance des risques, la traçabilité des évaluations et l'aide à la prise de décision. La plateforme développée permet notamment d'automatiser le calcul des scores de risque, de centraliser les données, de générer des rapports réglementaires et de renforcer le suivi des obligations de conformité. Déployée en environnement de production, elle démontre le potentiel des solutions numériques pour moderniser les dispositifs LBC/FT et améliorer l'efficacité opérationnelle des organisations soumises aux exigences réglementaires.

ABSTRACT

This dissertation presents the design and development of a centralized digital platform for Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) compliance risk assessment. Based on a rigorous methodology for analyzing the needs of regulatory compliance stakeholders, it describes how the combination of modern technologies such as multi-tenant SaaS architectures, business process automation, risk analysis, and centralized data management can meet the regulatory requirements of the sector.

This study highlights the contribution of information systems to improving risk governance, assessment traceability, and decision-making support. The developed platform enables the automation of risk score calculations, data centralization, regulatory report generation, and enhanced monitoring of compliance obligations. Deployed in a production environment, it demonstrates the potential of digital solutions to modernize AML/CFT frameworks and improve the operational efficiency of organizations subject to regulatory requirements.

À
MA FAMILLE

REMERCIEMENTS

Avant de commencer, nous tenons à exprimer notre profonde gratitude à ceux qui ont contribué à la réalisation de ce travail. Nous adressons nos sincères remerciements à nos responsables et encadrants, notamment :

- ◆ **Professeur KONATE Adama**, Directeur Général de l'ESATIC, qui dirige les équipes responsables de fournir une formation de haute qualité aux étudiants de cette prestigieuse institution ;
- ◆ **Dr (MC) SORO Étienne**, Directeur de la Pédagogie à l'ESATIC et son Équipe pour leur engagement à nous offrir un enseignement de qualité ;
- ◆ **Dr (MC) COULIBALY Kpinna Tiekoura** et **Dr GOLI CHARLES ETIENNE**, nos encadrants académiques pour leurs précieux conseils et le temps qu'il nous a généreusement accordé ;
- ◆ **Le corps professoral et l'ensemble du personnel administratif**, Pour la qualité des enseignements dispensés et le suivi tout au long de notre cursus ;
- ◆ **Monsieur TIEMOKO FRANCK OLIVIER**, Directeur général de NEXORA, pour son accueil, le temps et les efforts investis dans ce projet, ainsi que ses conseils et son expertise ;
- ◆ **Monsieur GILLES YAO, OTHNIEL YAO**, Respectivement Maître de stage et Responsables du département intelligence artificielle pour leur encadrement et assistance dans la réalisation de ce projet ;
- ◆ **Les familles AEEMCI-ESATIC**, pour leurs soutiens moraux et spirituels ;
- ◆ **Équipe NEXORA**, Équipe projet pour leur engagement et leur contribution essentielle à la réalisation de ce projet.

Nos sincères remerciements vont également à l'endroit de **notre famille, amis (es), camarades** et plus précisément à notre ami **KOUYATE Mamadou Moussa** pour nous avoir aidé à la réalisation de ce mémoire.

AVANTS-PROPOS

Ce rapport est rédigé dans le but d'obtenir le Master en Systèmes d'Information et Génie Logiciel (SIGL) de l'École Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC), à l'issue de notre parcours académique. Il présente les résultats d'une étude menée durant six (06) mois de stage au sein de l'entreprise NEXORA. Ce document porte sur la conception d'une plateforme numérique d'évaluation du risque de conformité réglementaire dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Ce stage nous a permis de mettre en pratique les compétences acquises au cours de notre formation, notamment en conception et développement d'applications web, en gestion des systèmes d'information ainsi qu'en automatisation des processus métier. Le projet vise à proposer une solution centralisée permettant d'évaluer, suivre et analyser les risques de conformité réglementaire conformément aux exigences liées à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Au cours de ce travail, plusieurs défis majeurs ont été rencontrés, notamment la conception d'une architecture applicative fiable et sécurisée, l'intégration de mécanismes de gestion et d'analyse des risques, la mise en place d'un système de traitement et de centralisation des données, ainsi que l'automatisation de certaines tâches grâce aux pratiques DevOps et aux processus CI/CD. Une attention particulière a également été portée à la sécurité, à la traçabilité des opérations et à l'optimisation des performances de la plateforme.

Grâce à des recherches approfondies, à l'exploitation de ressources documentaires pertinentes et à l'accompagnement de l'équipe technique de NEXORA, ces différents défis ont pu être progressivement surmontés. Le projet dispose actuellement d'une version web fonctionnelle et déjà déployée, permettant l'utilisation effective de la plateforme. En revanche, aucune version mobile n'a encore été développée à ce stade du projet.

Ce mémoire présente donc essentiellement le volet web de la plateforme, son architecture, ses fonctionnalités principales ainsi que les différentes technologies et méthodes utilisées pour sa réalisation.

SOMMAIRE

INTRODUCTION	1
CHAPITRE I : PRÉSENTATION DE L'ENTREPRISE	4
I. PRÉSENTATION DE LA STRUCTURE D'ACCUEIL (NEXORA)	4
II. ORGANISATION INTERNE DE NEXORA	5
CHAPITRE II : PRÉSENTATION DU PROJET	6
I. CADRE GÉNÉRAL DU PROJET	6
II. CONFORMITÉ RÉGLEMENTAIRE, BLANCHIMENT DES CAPITAUX ET FINANCEMENT DU TERRORISME	7
III. CAHIER DE CHARGE ET PLANIFICATION DES TÂCHES	8
CHAPITRE III : ÉTUDE DE L'EXISTANT ET ÉTAT DE L'ART	12
I. PRÉSENTATION DE L'EXISTANT ET SES LIMITES	12
II. ÉTAT DE L'ART	12
CHAPITRE IV : CONCEPTION DU MODÈLE D'ÉVALUATION DU RISQUE	18
I. IDENTIFICATION ET CLASSIFICATION DES CRITÈRES DE RISQUE	18
II. CONSTRUCTION DU MODÈLE DE SCORING DU RISQUE	21
III. APPROCHE MATHÉMATIQUE D'ÉVALUATION DU RISQUE	24
IV. MÉTHODES STATISTIQUES ET PROBABILISTES POUR L'AMÉLIORATION DU SCORING DE RISQUE	29
CHAPITRE V : CONCEPTION DE LA PLATEFORME	31
I. PRÉSENTATION DES MÉTHODES	31
II. ÉTUDE COMPARATIVE ET PRÉSENTATION DES MÉTHODES CHOISIES	32
CHAPITRE VI : RÉALISATIONS	33
I. DIAGRAMME DE CAS D'UTILISATION	33
II. DIAGRAMMES (SÉQUENCE, ACTIVITÉ, CLASSE)	36
CHAPITRE VII : RÉSULTATS	44
I. OUTILS ET TECHNOLOGIES UTILISÉS	44
II. PRÉSENTATION DES RÉSULTATS	47
III. DISCUSSION DES RÉSULTATS	58
CONCLUSION	63

LISTE DES SIGLES ET ACRONYMES

AML/CFT	: Anti-Money Laundering / Counter-Terrorist Financing
API	: Application Programming Interface
ARTCI	: Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire
BCEAO	: Banque Centrale des États de l'Afrique de l'Ouest
CENTIF	: Cellule Nationale de Traitement des Informations Financières
CI/CD	: Continuous Integration / Continuous Deployment (Intégration Continue / Déploiement Continu)
ENR	: Évaluation Nationale des Risques
ESATIC	: École Supérieure Africaine des Technologies de l'Information et de la Communication
FATF	: Financial Action Task Force (voir GAFI)
FCFA	: Franc de la Communauté Financière Africaine
FMI	: Fonds Monétaire International
GAFI	: Groupe d'Action Financière
GED	: Gestion Électronique des Documents
IA	: Intelligence Artificielle
JSON	: JavaScript Object Notation
JWT	: JSON Web Token
KYC	: Know Your Customer (Connaissance du Client)
LBC/FT	: Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme
MERISE	: Méthode d'Étude et de Réalisation Informatique par les Sous-Ensembles
OAPI	: Organisation Africaine de la Propriété Intellectuelle
OHADA	: Organisation pour l'Harmonisation en Afrique du Droit des Affaires
PME	: Petite et Moyenne Entreprise
PPE	: Personne Politiquement Exposée
RBAC	: Role-Based Access Control (Contrôle d'Accès Basé sur les Rôles)
SaaS	: Software as a Service (Logiciel en tant que Service)
SFD	: Système Financier Décentralisé
SMTP	: Simple Mail Transfer Protocol
UML	: Unified Modeling Language (Langage de Modélisation Unifié)
UEMOA	: Union Économique et Monétaire Ouest-Africaine
VPS	: Virtual Private Server (Serveur Privé Virtuel)

GLOSSAIRE

AML/CFT

Anti-Money Laundering / Counter-Terrorist Financing. Désignation anglophone de la LBC/FT. Ensemble des mécanismes réglementaires et opérationnels mis en œuvre pour prévenir le blanchiment des capitaux et le financement du terrorisme.

API (Application Programming Interface)

Interface de programmation applicative. Ensemble de règles et de protocoles permettant à deux systèmes informatiques de communiquer entre eux et d'échanger des données de manière standardisée.

Approche fondée sur les risques (AFR)

Méthode recommandée par le GAFI qui consiste à calibrer l'intensité des contrôles LBC/FT en fonction du niveau de risque identifié pour chaque client, produit, canal ou zone géographique.

Authentification JWT

Procédé de vérification d'identité reposant sur des jetons numériques signés (JSON Web Tokens). Le serveur émet un jeton lors de la connexion ; ce jeton est ensuite joint à chaque requête pour prouver l'identité de l'utilisateur.

Bénéficiaire effectif

Personne physique qui, en dernier ressort, possède ou contrôle une entité juridique ou pour le compte de laquelle une transaction est effectuée. L'identification du bénéficiaire effectif est une obligation fondamentale du KYC.

Blanchiment des capitaux

Processus visant à dissimuler l'origine illégale de fonds en leur donnant l'apparence de revenus légitimes. Il comprend généralement trois phases : le placement, l'empilage et l'intégration.

CI/CD (Intégration Continue / Déploiement Continu)

Ensemble de pratiques DevOps visant à automatiser l'intégration, les tests et le déploiement des modifications de code afin de réduire les cycles de livraison et d'améliorer la qualité des applications.

Conformité réglementaire

Respect par une organisation des lois, règlements, normes et directives qui encadrent son activité. Dans le domaine financier, elle englobe notamment les obligations LBC/FT, de protection des données et de reporting réglementaire.

Diagramme de cas d'utilisation

Représentation UML qui modélise les interactions entre les acteurs (utilisateurs ou systèmes) et les fonctionnalités d'un système logiciel. Il décrit ce que le système fait, sans préciser comment il le fait.

Diagramme de classes

Représentation UML qui décrit la structure statique d'un système en montrant ses classes, leurs attributs, méthodes et les relations (héritage, association, composition) qui les unissent.

Diagramme de séquence

Représentation UML qui montre les interactions entre objets ou composants au cours du temps pour réaliser un scénario donné. Il illustre l'ordre chronologique des échanges de messages.

Évaluation Nationale des Risques (ENR)

Exercice mené à l'échelle d'un pays pour identifier et évaluer les risques de blanchiment de capitaux et de financement du terrorisme. En Côte d'Ivoire, l'ENR réalisée en 2019 a servi de référence pour le dispositif LBC/FT national.

Financement du terrorisme

Collecte, mise à disposition ou gestion de fonds destinés à financer des actes terroristes ou des organisations terroristes, que ces fonds soient d'origine légale ou illégale.

Firme

Unité économique à caractère commercial ou industriel, organisée pour produire des biens ou des services en vue de réaliser un profit. Dans le contexte de cette plateforme, le terme désigne les cabinets et institutions financiers utilisant la solution.

GAFI (Groupe d'Action Financière)

Organisation intergouvernementale créée en 1989 qui définit les normes internationales de lutte contre le blanchiment des capitaux, le financement du terrorisme et la prolifération. Ses recommandations constituent la référence mondiale en matière de LBC/FT.

KYC (Know Your Customer)

Procédure de vérification de l'identité des clients, destinée à évaluer leur profil de risque avant et pendant la relation d'affaires. Elle comprend la collecte des informations d'identité, la vérification des documents, l'identification des bénéficiaires effectifs et l'évaluation du risque.

LBC/FT

Lutte contre le Blanchiment des Capitaux et le Financement du Terrorisme. Ensemble des mesures légales, réglementaires et opérationnelles visant à détecter, prévenir et réprimer le blanchiment et le financement du terrorisme.

MERISE

Méthode d'analyse et de conception des systèmes d'information développée en France dans les années 1970-1980. Elle distingue les niveaux conceptuel, logique et physique et s'appuie notamment sur le Modèle Conceptuel des Données (MCD) et le Modèle Conceptuel des Traitements (MCT).

MongoDB

Système de gestion de base de données NoSQL orienté documents. Il stocke les données sous forme de documents JSON (BSON), offrant flexibilité de schéma et performances élevées pour les données hiérarchiques ou variables.

Multi-tenant

Architecture logicielle dans laquelle une seule instance d'une application sert plusieurs clients (tenants) simultanément, tout en maintenant une isolation stricte de leurs données et configurations respectives.

NestJS

Framework Node.js basé sur TypeScript, inspiré d'Angular, permettant de construire des applications côté serveur robustes et maintenables grâce à une architecture modulaire et à l'injection de dépendances.

PPE (Personne Politiquement Exposée)

Individu qui occupe ou a occupé une fonction publique importante (chef d'État, membre du gouvernement, dirigeant d'une institution internationale, etc.). Les PPE font l'objet d'une vigilance renforcée dans le cadre du KYC en raison de leur exposition accrue aux risques de corruption et de blanchiment.

RBAC (Role-Based Access Control)

Modèle de contrôle d'accès dans lequel les droits d'accès aux ressources d'un système sont attribués en fonction des rôles assignés aux utilisateurs, et non directement à des individus.

SaaS (Software as a Service)

Modèle de distribution logicielle dans lequel l'application est hébergée par le fournisseur et accessible aux utilisateurs via Internet, éliminant le besoin d'installation locale et simplifiant la maintenance.

Score de risque

Valeur numérique (généralement de 1 à 4) attribuée à un client, un produit ou une opération pour quantifier son niveau de risque LBC/FT. Il résulte de l'évaluation pondérée de plusieurs critères de risque.

SFD (Système Financier Décentralisé)

Institution de microfinance, mutuelle d'épargne et de crédit ou coopérative financière offrant des services financiers aux populations non bancarisées. Les SFD sont soumis aux obligations LBC/FT au même titre que les banques.

Snapshot (instantané)

Copie figée de l'état d'un système ou d'une donnée à un instant précis. Dans le contexte de la plateforme, le versioning des barèmes de risque par snapshot garantit que les évaluations historiques conservent les critères en vigueur à la date de leur réalisation.

UML (Unified Modeling Language)

Langage de modélisation graphique standardisé par l'OMG, utilisé pour spécifier, visualiser, construire et documenter les artefacts d'un système logiciel. Il comprend plusieurs types de diagrammes structurels et comportementaux.

Vulnérabilité

Dans le modèle d'évaluation du risque LBC/FT, la vulnérabilité désigne les faiblesses internes d'une organisation ou d'un secteur qui pourraient être exploitées à des fins de blanchiment. Elle est croisée avec le score de menace pour déterminer le risque global.

LISTE DES FIGURES

Figure 1 - Organigramme de DEKKO Group	5
Figure 2 - Diagramme de Gantt.....	11
Figure 3 - Arbre Hiérarchique des Critères de Risque: Domaine Clients	19
Figure 4 - Arbre Hiérarchique des Critères de Risque Domaine : Zone _geo	20
Figure 5 - Arbre Hiérarchique des Critères de Risque Domaine : Produits_ser	20
Figure 6 - Arbre Hiérarchique des Critères de Risque Domaine : Canaux	20
Figure 7 - Processus de Scoring du Risque — Vue d'ensemble.....	23
Figure 8 - Modèle Mathématique d'Évaluation du Risque — Synthèse	28
Figure 9 - Illustration du Processus Unifié (UP).....	31
Figure 10 - Illustration du langage UML	31
Figure 11 - Illustration de la méthode MERISE.....	32
Figure 12 - Diagramme de cas d'utilisation.....	33
Figure 13 - Diagramme de Séquence, Authentification (Login).....	36
Figure 14 - Diagramme de Séquence, Création d'un Utilisateur.....	37
Figure 15 - Diagramme de Séquence, Évaluation KYC avec Calcul de Risque.....	38
Figure 16 - Diagramme de Séquence, Mot de Passe Oublié	39
Figure 17 - Diagramme d'activité, Processus d'Authentification	40
Figure 18 - Diagramme d'Activité, Création de Client (Workflow 3 Étapes).....	41
Figure 19 - Diagramme de classes	42
Figure 20 - Landing page	52
Figure 21 - Page d'authentification.....	53
Figure 22 - Page tableau de bord.....	53
Figure 23 - Visualisation de la liste des clients	54
Figure 24 - Visualisation des détails d'un client.....	54
Figure 25 - Visualisation des détails de l'évaluation d'un client	55
Figure 26 - La matrice de croisement Vulnérabilité x Menace	55
Figure 27 - Page de création de formulaires KYC dynamiques	56
Figure 28 - Page d'abonnement pour un cabinet	57
Figure 29 - Les 4 piliers réglementaires GIABA	57

LISTE DES TABLEAUX

Tableau 1 - Tableau représentatif des domaines de risque.....	18
Tableau 2 - Tableau des types de noeuds	19
Tableau 3 - Tableau des niveaux de risque	21
Tableau 4 – Tableau de la collection kyc_evaluations	22
Tableau 5 - Tableau de symboles	24
Tableau 6 - Tableau de la matrice de croisement Vulnérabilité × Menace	25
Tableau 7 - Tableau du label de risque final	25
Tableau 8 - Tableau de données d'entrée	26
Tableau 9 - Tableau comparatif UML - MERISE.....	32
Tableau 10 - Cas d'utilisation : s'authentifier	34
Tableau 11 - Cas d'utilisation : Créer un client (workflow à 3 étapes)	34
Tableau 12 - Cas d'utilisation : Créer une évaluation KYC	35
Tableau 13 - Tableau récapitulatif du matériel utilisé.....	46
Tableau 14 - Tableau des modules fonctionnels	48
Tableau 15 - Tableau des acteurs du système	49
Tableau 16 - Tableau récapitulatif des infrastructures et de leurs prix	58

INTRODUCTION

La lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) constitue aujourd'hui un enjeu majeur pour la stabilité des systèmes financiers et économiques. Selon le Fonds Monétaire International, les flux financiers illicites représentent entre 2 % et 5 % du produit intérieur brut mondial, soit entre 800 milliards et 2 000 milliards de dollars américains chaque année (Fonds Monétaire International, 2024). Face à cette menace, la communauté internationale a progressivement renforcé son cadre réglementaire à travers les recommandations du Groupe d'Action Financière (GAFI), qui constituent aujourd'hui la référence mondiale en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (Groupe d'Action Financière, 2023).

En Afrique de l'Ouest, plusieurs pays demeurent confrontés à des insuffisances liées à la gestion et à l'évaluation des risques de conformité (Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest, 2023). La Côte d'Ivoire n'échappe pas à cette réalité. L'Évaluation Nationale des Risques (ENR) réalisée en 2019 a révélé un niveau de risque moyennement élevé en matière de blanchiment de capitaux et un niveau élevé concernant le financement du terrorisme (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019). Dans de nombreuses organisations, les évaluations reposent encore sur des traitements manuels réalisés à l'aide de fichiers Excel, entraînant des difficultés de centralisation, des risques d'erreurs et un manque de traçabilité des opérations (Banque Mondiale, 2022). L'adoption de solutions numériques innovantes apparaît ainsi comme une nécessité pour améliorer l'efficacité des dispositifs de conformité et répondre aux exigences réglementaires croissantes. La Banque Centrale des États de l'Afrique de l'Ouest (BCEAO) a d'ailleurs encouragé les institutions financières de la zone UEMOA à accélérer leur transformation numérique, notamment en matière de conformité réglementaire, afin de répondre plus efficacement aux exigences croissantes des standards internationaux (Banque centrale des États de l'Afrique de l'Ouest, 2025). (Groupe d'Action Financière, 2023)

C'est dans ce contexte que l'entreprise NEXORA nous a confié le thème : « **CONCEPTION D'UNE PLATEFORME NUMÉRIQUE D'ÉVALUATION DU RISQUE DE CONFORMITÉ RÉGLEMENTAIRE : CAS DE LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME** ». Ce projet vise à concevoir et développer une solution centralisée permettant d'automatiser les

évaluations de risques, de centraliser les données, d'améliorer la traçabilité des opérations et de faciliter la production de rapports destinés à l'aide à la décision.

Au regard de ces objectifs, plusieurs questions se posent : comment concevoir une plateforme capable d'automatiser efficacement l'évaluation des risques de conformité ? Comment centraliser et sécuriser les données tout en garantissant leur confidentialité ? Quels mécanismes mettre en œuvre pour assurer la traçabilité des évaluations et faciliter la production de rapports réglementaires ?

Le présent mémoire se propose d'analyser les résultats obtenus à l'issue de ce projet. Il s'agit d'évaluer dans quelle mesure la plateforme développée répond aux objectifs fixés, d'identifier ses apports sur les plans métier, technique et organisationnel, de mettre en évidence les limites rencontrées et d'explorer les perspectives d'évolution susceptibles de renforcer ses capacités, notamment par l'intégration de méthodes avancées d'analyse des risques et de techniques d'intelligence artificielle.

PREMIÈRE PARTIE: GÉNÉRALITÉ ET CONTEXTE

*Dans cette première partie, il s'agira de faire une
brève présentation de la structure d'accueil et
d'une étude préalable du projet*

CHAPITRE I : PRÉSENTATION DE L'ENTREPRISE

Dans ce chapitre, nous effectuons une présentation de l'organisme d'accueil, ses missions et compétences.

I. PRÉSENTATION DE LA STRUCTURE D'ACCUEIL (NEXORA)

1. Présentation de DEKKO Group

DEKKO Group est un groupe ivoirien spécialisé dans l'accompagnement et le développement entrepreneurial. Fondé par Monsieur **Désiré KONAN**, expert-comptable diplômé, le groupe a son siège à Abidjan, Cocody II Plateaux. Il a pour devise : « Nous transformons vos rêves en succès ».

La société mère est une société anonyme avec un conseil d'administration disposant d'un capital de 1 000 millions de F CFA, ce qui reflète sa solidité et sa capacité à développer des activités à forte valeur ajoutée. Le groupe dispose également d'une présence en ligne à travers son site officiel, qui présente ses activités et ses filiales.

Le groupe est organisé autour de plusieurs entités complémentaires qui interviennent dans différents domaines, réparties en trois pôles complémentaires, notamment :

- **Pôle Consultance et Expertise (CERCLE):** comprend **CERCLE Compta** (expertise comptable et audit), **CERCLE Conseil** (conseil juridique, fiscal, social et ressources humaines) et **CERCLE Deals** (incubation et développement commercial). La marque **CERCLE** a été initiée en 2003 par **M. Désiré KONAN** ;
- **Pôle Hôtellerie d'Affaires (KAY):** regroupe **KAY Immobilier** (gestion foncière), **KAY Hospitality** (centre d'affaires, résidences meublées, domiciliation) et **KAY Services** (maintenance, nettoyage et sécurité) ;
- **Pôle Support:** comprend **NEXORA** (transformation digitale, cybersécurité, intelligence artificielle) ainsi que le Fonds de Solidarité DEKKO, mutuelle sociale du groupe.

2. Historique et mission

DEKKO Group trouve son origine en 2003 avec la création de la marque **CERCLE** (« Conseil Expert pour le Renforcement des Capacités et la Libre Entreprise »). Cette structure a constitué la base du développement du groupe, qui s'est progressivement diversifié autour de plusieurs activités liées à l'accompagnement des entreprises et à la promotion de l'entrepreneuriat. La marque **CERCLE** est enregistrée auprès de l'OAPI, garantissant ainsi sa reconnaissance juridique.

Au fil de son évolution, DEKKO Group a renforcé son positionnement en Côte d'Ivoire, notamment avec l'agrément de KAY CENTER comme premier centre d'affaires reconnu par le Ministère de la Promotion des PME en 2020. Aujourd'hui, le groupe a pour mission d'accompagner les entrepreneurs, les PME et les entreprises à travers des services variés favorisant leur croissance et leur transformation.

II. ORGANISATION INTERNE DE NEXORA

1. NEXORA, centre d'accueil

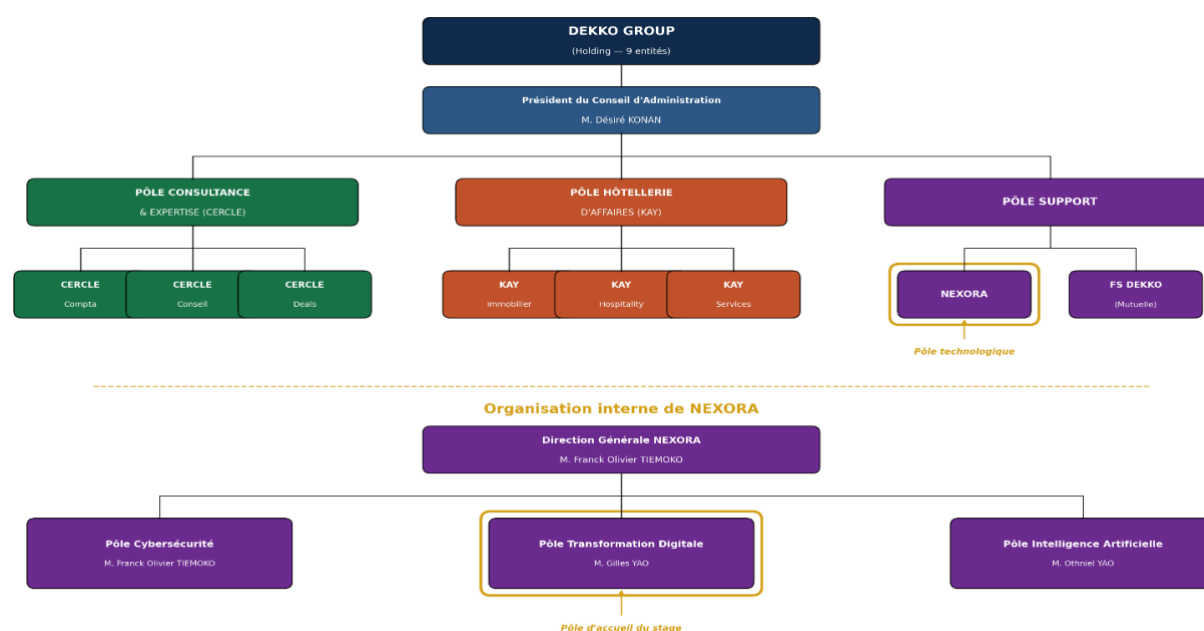
Bien que récente, NEXORA a rapidement structuré ses activités autour de trois principaux domaines en cohérence avec sa vision :

- le pôle Cybersécurité assure la protection des systèmes des entreprises clientes à travers des audits, des analyses de vulnérabilités et des actions de sensibilisation face aux cybermenaces ;
- le pôle Transformation Digitale accompagne les organisations dans leur transition numérique en proposant des solutions adaptées à leurs besoins et à leur environnement ;
- le pôle Intelligence Artificielle constitue le centre d'innovation du groupe, avec le développement de solutions basées sur l'IA telles que l'automatisation, l'analyse prédictive et les systèmes de recommandation.

L'ensemble des équipes travaille selon une méthodologie Agile (Scrum), organisée en cycles courts afin de favoriser l'amélioration continue et une évolution rapide des projets.

2. Organigramme de DEKKO Group

L'organigramme de DEKKO Group est présenté sur la figure ci-contre :



CHAPITRE II : PRÉSENTATION DU PROJET

Dans ce chapitre, nous effectuons une présentation de l'existant de laquelle découle la rédaction du cahier des charges.

I. CADRE GÉNÉRAL DU PROJET

1. Contexte et justifications

La lutte contre le blanchiment de capitaux et le financement du terrorisme constitue aujourd'hui un enjeu majeur pour les institutions financières et les autorités de régulation. En Côte d'Ivoire, l'Évaluation Nationale des Risques (ENR) réalisée en 2019 a révélé que le pays présente un niveau de risque moyennement élevé en matière de blanchiment de capitaux et un niveau élevé concernant le financement du terrorisme (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019).

Cette évaluation a également mis en évidence plusieurs insuffisances dans le dispositif actuel de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Parmi les principales faiblesses relevées figurent le manque d'interconnexion des systèmes d'information, l'insuffisance des ressources techniques et humaines, l'absence de mécanismes efficaces de coopération entre administrations ainsi que les difficultés liées à l'identification et à la détection des opérations suspectes (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019).

Dans la pratique, les processus d'évaluation des risques reposent encore fortement sur des traitements manuels réalisés à l'aide de fichiers Excel. Cette méthode rend les analyses longues, complexes et exposées aux erreurs humaines. De plus, l'exploitation des données reste limitée face au volume important d'informations à traiter provenant de plusieurs secteurs tels que les banques, les assurances, les systèmes financiers décentralisés ou encore les administrations publiques (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019).

Face à ces constats, la mise en place d'une plateforme intelligente d'analyse et d'évaluation des risques apparaît comme une nécessité. Le projet vise ainsi à proposer une solution numérique centralisée capable d'automatiser les évaluations, d'améliorer l'analyse des données et de faciliter la détection des vulnérabilités liées au blanchiment de capitaux et au financement du terrorisme.

2. Objectifs du projet

L'objectif principal de ce projet est de concevoir et développer une plateforme intelligente de gestion et d'évaluation des risques liés au blanchiment de capitaux et au financement du

terrorisme. Ce qui implique plusieurs sous-objectifs, à savoir centraliser les données provenant des différents secteurs concernés, automatiser le processus d'évaluation des risques, réduire les erreurs liées aux traitements manuels, améliorer l'analyse des données grâce à des outils intelligents, faciliter la détection des anomalies et opérations suspectes, produire des rapports et tableaux de bord dynamiques pour l'aide à la décision, renforcer le suivi des indicateurs de conformité et de vulnérabilité, mais aussi améliorer la rapidité, la fiabilité et la traçabilité des évaluations.

Cette solution permettra ainsi d'optimiser le processus d'analyse des risques tout en modernisant le dispositif actuel grâce à l'intégration de technologies numériques et d'outils d'intelligence artificielle.

II. CONFORMITÉ RÉGLEMENTAIRE, BLANCHIMENT DES CAPITAUX ET FINANCEMENT DU TERRORISME

1. La conformité réglementaire

La conformité réglementaire désigne l'ensemble des mesures mises en œuvre par une organisation afin de respecter les lois, règlements et normes applicables à son activité. Dans le secteur financier, elle vise principalement à prévenir les risques liés au blanchiment des capitaux, au financement du terrorisme et à la criminalité financière.

À l'échelle internationale, les exigences de conformité reposent principalement sur les recommandations du Groupe d'Action Financière (GAFI), qui constituent la référence mondiale en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme. Ces recommandations imposent notamment l'identification des clients, l'évaluation des risques, la surveillance des transactions et la conservation des informations de conformité ((FATF), 2025). En Côte d'Ivoire, ces exigences sont encadrées par l'Ordonnance n°2023-875 du 23 novembre 2023 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la prolifération des armes de destruction massive, qui s'inscrit dans le cadre de la loi uniforme adoptée par l'UEMOA (République de Côte d'Ivoire, 2023).

2. Le blanchiment des capitaux

Le blanchiment des capitaux est le processus qui consiste à dissimuler l'origine illicite de fonds provenant d'activités criminelles afin de leur donner une apparence légale. Selon les standards internationaux, ce phénomène compromet l'intégrité du système financier et favorise le développement de la criminalité organisée. Le blanchiment est généralement présenté en trois étapes : le placement des fonds dans le système financier, leur dissimulation à travers plusieurs opérations financières (empilement ou *layering*), puis leur réintégration dans l'économie légale

(intégration). Cette approche est aujourd'hui reconnue par les organismes internationaux de lutte contre la criminalité financière. (Fonds Monétaire International (FMI), 2025).

3. Le financement du terrorisme

Le financement du terrorisme consiste à fournir, collecter ou transférer des fonds destinés à soutenir des activités terroristes ou des organisations terroristes. Contrairement au blanchiment des capitaux, les ressources utilisées peuvent provenir aussi bien d'activités légales qu'illégales. L'objectif est donc d'identifier la destination des fonds plutôt que leur origine (Fonds Monétaire International (FMI), 2025).

Face à cette menace, le GAFI recommande une approche fondée sur le risque permettant aux institutions financières et aux organismes de conformité de concentrer leurs efforts sur les clients, secteurs ou opérations présentant les niveaux de risque les plus élevés. Cette approche constitue aujourd'hui le fondement des systèmes modernes d'évaluation du risque de conformité ((FATF), 2025).

III. CAHIER DE CHARGE ET PLANIFICATION DES TÂCHES

L'apport du cahier de charges est crucial pour tout projet informatique. Ce dernier permet de récapituler les différents besoins liés au projet, il détaille les fonctionnalités requises pour l'application à mettre en place. Il comprend les besoins fonctionnels, qui sont les différentes fonctionnalités l'application, ainsi que les besoins non-fonctionnels, qui se concentrent sur les exigences et les contraintes du projet.

1. Les besoins fonctionnels

Les besoins fonctionnels décrivent les services que la plateforme doit fournir aux différents acteurs du système

1.1.Gestion des utilisateurs et des accès

- Authentification sécurisée des utilisateurs.
- Gestion des sessions utilisateur.
- Gestion des rôles et des droits d'accès (Super Administrateur, Administrateur, Initiateur, Documentaliste, Responsable de la conformité).
- Inscription et récupération de mot de passe.
- Contrôle d'accès aux différentes fonctionnalités selon le profil utilisateur.

1.2.Gestion des cabinets (Mode SaaS)

- Création et administration des cabinets.
- Gestion des abonnements et licences.
- Gestion multi-tenant des différents cabinets.

- Paramétrage des informations propres à chaque cabinet.

1.3.Gestion des dossiers clients KYC

- Création des dossiers clients.
- Consultation, modification et mise à jour des informations clients.
- Gestion des personnes physiques, personnes morales et personnes politiquement influentes.
- Gestion des bénéficiaires effectifs et dirigeants.
- Consultation de l'historique des évaluations.

1.4.Gestion des dossiers et du processus KYC

- Création, mise à jour et suivi des dossiers clients KYC.
- Gestion des formulaires dynamiques, des documents justificatifs et des référentiels de risque.
- Vérification, validation et archivage des informations de conformité.

1.5.Évaluation du risque et contrôle de conformité

- Calcul des scores de menace, de vulnérabilité et du niveau global de risque.
- Vérification de la cohérence entre les informations déclarées et les pièces justificatives, avec détection des anomalies.
- Recalcul et historisation des évaluations après revue documentaire afin d'assurer la traçabilité et la fiabilité des décisions de conformité.

1.6.Archivage, traçabilité et reporting

- Archivage des dossiers KYC.
- Conservation des différentes versions des dossiers.
- Consultation des archives historiques et des dossiers nécessitant une réévaluation.
- Traçabilité complète des évaluations et modifications.
- Visualisation des indicateurs clés de conformité.
- Cartographie des risques du portefeuille clients.
- Segmentation des clients selon leur niveau de risque.
- Génération de rapports d'analyse et de conformité.

2. Besoins non fonctionnels

Les besoins non fonctionnels définissent les contraintes de qualité, de performance et de sécurité auxquelles la plateforme doit répondre.

2.1.Sécurité et confidentialité

- Authentification sécurisée par JWT et contrôle d'accès par rôle (RBAC).

- Protection et chiffrement des données sensibles via HTTPS/TLS.
- Respect des exigences réglementaires (LBC/FT) et des bonnes pratiques de sécurité.
- Journalisation des actions utilisateurs.

2.2.Performance et disponibilité

- Temps de réponse optimisés maximum 3 secondes près.
- Haute disponibilité de la plateforme.
- Sauvegarde et restauration des données.

2.3.Évolutivité et maintenabilité

- Architecture modulaire et évolutive.
- Compatibilité avec les navigateurs modernes.
- Maintenabilité du code source.
- Intégration des pratiques DevOps et CI/CD pour le déploiement.

3. Livrables

Un livrable est tout élément concret que l'équipe projet doit fournir au client ou à l'encadrant à la fin d'une phase ou du projet.

3.1.Livrables de conception

- Cahier des charges validé.
- Modèle de données et dossier d'architecture technique.
- Maquettes des interfaces utilisateur.

3.2.Livrables de réalisation

- Plateforme web ALM/KYC fonctionnelle.
- API et base de données opérationnelles.
- Modules d'évaluation et de gestion du risque implémentés.

3.3.Livrables de validation et d'exploitation

- Rapports de tests et procès-verbal de recette.
- Documentation technique et guide utilisateur.
- Plateforme déployée et mise en production.

4. Planification des tâches

Le diagramme de Gantt présente le planning d'exécution du projet.

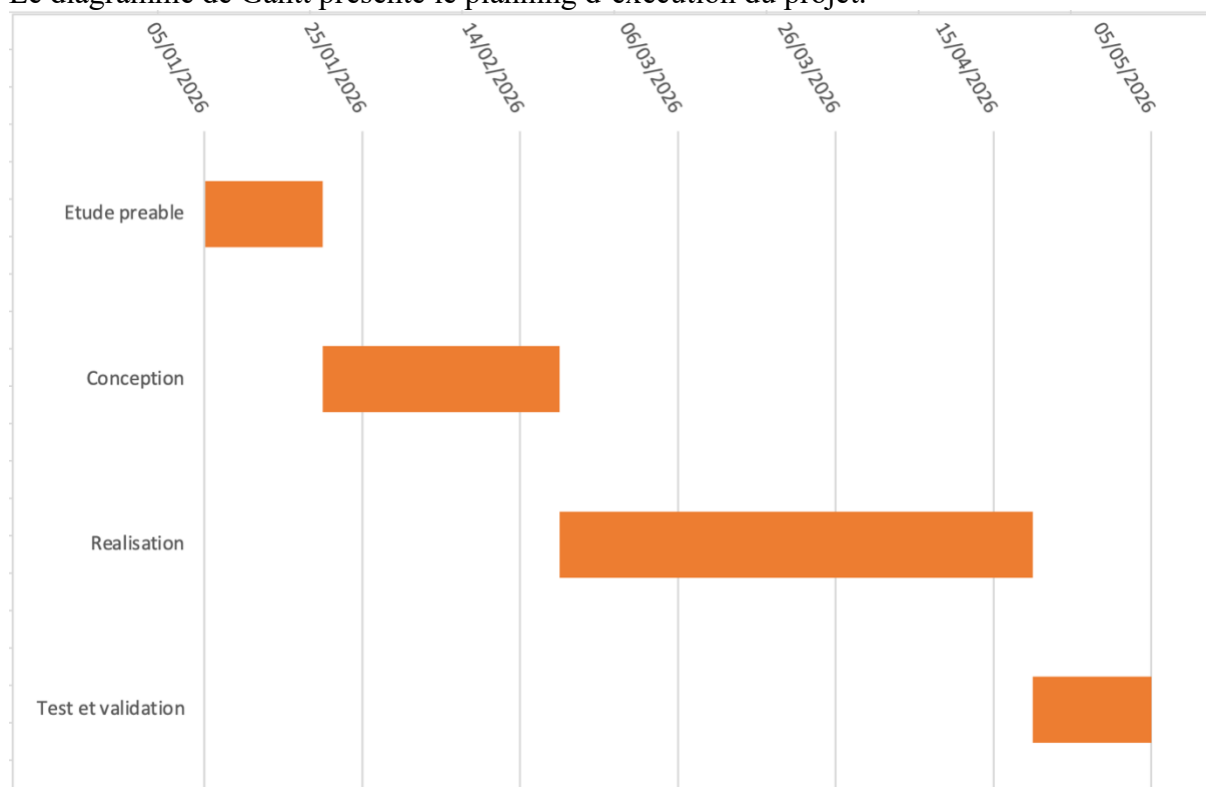


Figure 2 - Diagramme de Gantt

CHAPITRE III : ÉTUDE DE L'EXISTANT ET ÉTAT DE L'ART

Ce chapitre est consacré à l'étude de l'existant et à l'état de l'art. Il présente les solutions, méthodes et outils déjà développés dans le domaine concerné, tout en mettant en lumière leurs forces et leurs limites. Cette analyse permet de justifier les choix effectués pour la conception de notre solution.

I. PRÉSENTATION DE L'EXISTANT ET SES LIMITES

1. Présentation de l'existant

L'existant repose principalement sur une méthode d'évaluation basée sur des traitements manuels et des outils bureautiques, notamment des fichiers Excel utilisés pour le calcul des scores de menace et de vulnérabilité. Les données sont collectées auprès de plusieurs structures puis analysées selon des critères définis par la méthodologie de la Banque Mondiale adoptée par la Côte d'Ivoire (Banque Mondiale, 2015).

Le système actuel permet d'obtenir des résultats sectoriels et nationaux concernant les niveaux de risque.

2. Limites de l'existant

Toutefois, plusieurs limites importantes ont été identifiées. Premièrement, l'absence d'interconnexion entre les systèmes d'information des différentes administrations ralentit les échanges de données et réduit l'efficacité des analyses (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019). Deuxièmement, les traitements manuels augmentent les risques d'erreurs, de duplication et de perte d'informations. Troisièmement, les capacités actuelles ne permettent pas une exploitation intelligente et dynamique des données en temps réel.

Par ailleurs, plusieurs secteurs présentent des difficultés liées à la détection automatique des opérations suspectes, à l'identification des bénéficiaires effectifs et à la centralisation des informations (République de Côte d'Ivoire, Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme, 2019). Les insuffisances en matière de conformité, de supervision et de suivi des indicateurs de risque rendent également le processus d'évaluation moins performant. Enfin, le volume important de données à analyser rend l'utilisation exclusive des fichiers Excel peu adaptée aux besoins actuels de suivi et d'analyse avancée.

II. ÉTAT DE L'ART

1. La lutte contre le blanchiment de capitaux et le financement du terrorisme

La lutte contre le blanchiment de capitaux et le financement du terrorisme, appelée LBC/FT, regroupe l'ensemble des mesures destinées à empêcher l'utilisation du système financier à des fins criminelles. Le blanchiment consiste à donner une apparence légale à des fonds d'origine

illégale, tandis que le financement du terrorisme vise à fournir des ressources financières à des personnes ou à des groupes impliqués dans des actes terroristes. Ces deux phénomènes représentent une menace pour la stabilité économique, la sécurité des États et la confiance dans les institutions financières (Fonds monétaire international, 2023).

Le cadre international de référence le plus connu est celui du Groupe d'action financière, ou GAFI. Le GAFI recommande aux pays de mettre en place des mesures de prévention, de contrôle et de sanction adaptées au niveau de risque. L'un de ses principes essentiels est l'approche fondée sur les risques, qui consiste à renforcer les contrôles lorsque le risque est élevé et à les adapter lorsque le risque est faible. Cette logique est aujourd'hui au cœur de la conformité LBC/FT dans la plupart des systèmes financiers modernes. En Côte d'Ivoire, la CENTIF joue un rôle important dans ce dispositif. Elle reçoit et analyse les déclarations de soupçon transmises par les professionnels assujettis. Son action montre que la conformité ne dépend pas seulement des textes, mais aussi de la capacité des organisations à collecter, vérifier et conserver les informations de manière fiable (Centre d'Information Financière de Côte d'Ivoire, n.d.).

2. Le processus KYC et l'évaluation du risque client

Le KYC, pour "Know Your Customer", est une étape essentielle de la conformité. Il consiste à identifier le client, vérifier son identité, comprendre son activité et apprécier la nature de la relation d'affaires. Cette démarche concerne aussi bien les personnes physiques que les personnes morales. Elle permet de réduire les risques liés à l'usurpation d'identité, à la fraude et à l'utilisation de sociétés écrans (Fonds monétaire international, 2023).

Dans les recommandations internationales, le KYC n'est pas une formalité administrative. Il s'agit d'un processus de vigilance continue, qui doit être actualisé tout au long de la relation avec le client. L'évaluation du risque prend en compte plusieurs éléments comme le pays, le secteur d'activité, les opérations inhabituelles, la structure de propriété et le comportement du client. Cette évaluation permet d'appliquer des contrôles plus forts aux dossiers sensibles (Centre d'Information Financière de Côte d'Ivoire, n.d.).

3. La digitalisation de la conformité et l'apport des plateformes SaaS

La digitalisation de la conformité consiste à utiliser des outils numériques pour automatiser, centraliser et tracer les activités de contrôle. Dans le domaine de la LBC/FT, cette évolution est importante, car les organisations ont besoin de traiter beaucoup d'informations, de garder des preuves, et de produire rapidement des rapports en cas de contrôle. Les outils numériques permettent donc de gagner du temps, de réduire les erreurs et d'améliorer la qualité de la surveillance (Banque centrale des États de l'Afrique de l'Ouest, 2025).

Les plateformes SaaS sont particulièrement adaptées à ce besoin. Elles permettent d'accéder à un service via Internet, sans installation lourde, et de mutualiser l'infrastructure entre plusieurs utilisateurs ou plusieurs structures. Le modèle multi-tenant est intéressant pour les cabinets et les institutions financières, car il permet d'avoir une seule plateforme pour plusieurs clients tout en gardant une séparation stricte des données (Amazon Web Service, 2024).

Cette architecture réduit les coûts, simplifie la maintenance et facilite les mises à jour. Elle est aussi utile pour proposer un service scalable, c'est-à-dire capable de grandir avec le nombre d'utilisateurs et de dossiers à traiter. Dans le cas de la plateforme LBCFT, cela permet de gérer plusieurs cabinets, chacun avec ses propres données, ses propres utilisateurs et ses propres abonnements (Signiant, 2025).

4. Les solutions existantes de conformité LBC/FT

4.1. Les solutions d'automatisation du KYC

Certaines plateformes se concentrent d'abord sur le **KYC**, c'est-à-dire la collecte et la vérification des informations du client. Elles permettent d'enregistrer les données d'identité, de vérifier les documents fournis et de centraliser les éléments du dossier dans un espace unique. L'objectif principal est de réduire le traitement manuel et d'aider les équipes de conformité à constituer un dossier client plus rapidement et de manière plus structurée (ComplyAdvantage, 2024).

Ces solutions vont souvent plus loin en proposant un suivi des pièces justificatives et une actualisation des informations client au cours de la relation d'affaires. Elles sont donc utiles pour les organisations qui veulent garder un dossier à jour et limiter les erreurs de saisie. Toutefois, elles restent souvent centrées sur la collecte et la vérification, sans toujours proposer une vraie méthode d'évaluation du risque adaptée au contexte local (ChapsVision, n.d.).

4.2. Les solutions de screening et de surveillance

D'autres plateformes sont spécialisées dans le **screening**, c'est-à-dire la vérification du client contre des listes de sanctions, des listes de personnes politiquement exposées (PPE) ou d'autres bases de référence. Elles servent à détecter rapidement si un client, un bénéficiaire effectif ou une transaction présente un signal d'alerte. Ce type d'outil est très utile pour repérer les situations sensibles avant l'entrée en relation ou pendant le suivi d'un dossier (ComplyAdvantage, 2024).

Ces solutions incluent aussi souvent une fonction de **surveillance continue**. Cela signifie qu'elles analysent les opérations ou les profils à mesure que de nouvelles informations apparaissent, afin de signaler les anomalies ou les changements de risque. Elles sont donc très efficaces pour les grandes organisations qui traitent un volume important de dossiers. En

revanche, elles sont parfois complexes à paramétrer et peuvent dépasser les besoins ou les moyens de petites structures (ChapsVision, n.d.).

4.3. Les solutions orientées analyse du risque

Certaines plateformes ne se limitent pas au KYC ou au screening ; elles intègrent aussi des outils d'**analyse du risque**. Leur rôle est d'aider les équipes à classer les clients selon un niveau de risque défini à partir de critères comme le pays, l'activité, la structure de l'entreprise ou le comportement observé. Ces outils permettent de prioriser les contrôles et de réserver plus d'attention aux dossiers les plus sensibles (ComplyAdvantage, 2024).

Dans la pratique, ces systèmes fonctionnent souvent avec des règles internes, des scores ou des alertes automatiques. Ils sont utiles pour homogénéiser les décisions et soutenir le travail de conformité. Cependant, ils ne sont pas toujours conçus pour intégrer des critères réglementaires locaux ou des méthodes d'évaluation simples et directement compréhensibles par des cabinets de taille moyenne (ChapsVision, n.d.).

4.4. Les solutions de gestion documentaire et de traçabilité

Une autre catégorie de solutions vise surtout la **conservation des preuves** et la **traçabilité**. Elles permettent d'archiver les documents KYC, les justificatifs, les évaluations de risque et les décisions prises par les utilisateurs. Leur intérêt principal est de faciliter les contrôles internes et les audits externes, car elles gardent une trace de toutes les actions réalisées sur un dossier (Expertise France, 2024).

Ces outils sont essentiels dans un environnement réglementaire strict, parce qu'ils permettent de démontrer qu'une organisation a bien appliqué ses obligations de conformité. Mais ils restent souvent centrés sur le stockage des documents, sans offrir à eux seuls une logique complète de classification du risque, de gestion multi-cabinets et d'automatisation métier (Expertise France, 2024).

4.5. Limites des solutions existantes

Même si ces solutions sont utiles, elles ne couvrent pas toujours l'ensemble des besoins d'une structure comme celle visée par le projet LBCFT. Beaucoup sont pensées pour des marchés internationaux, avec des coûts plus élevés, une forte dépendance au cloud étranger et une configuration parfois trop complexe pour des cabinets locaux. Elles répondent donc à une partie du besoin, mais pas à l'ensemble du besoin (ComplyAdvantage, 2024).

Dans le contexte africain et ivoirien, il existe un besoin pour une solution plus simple, plus accessible et plus adaptée aux pratiques réelles des cabinets de conseil, des cabinets comptables et des institutions financières. C'est précisément ce vide que le projet LBCFT cherche à

combler, en proposant une plateforme SaaS multi-tenant qui réunit le KYC, l'évaluation du risque, l'archivage et la gestion de plusieurs cabinets dans un même système.

DEUXIÈME PARTIE : ÉTUDE THÉORIQUE ET TECHNIQUE DU SYSTÈME

Dans cette partie nous vous présentons la méthode d'analyse et de conception utilisée ainsi que les différents diagrammes décrivant la conception du système

CHAPITRE IV : CONCEPTION DU MODÈLE D'ÉVALUATION DU RISQUE

Ce chapitre présente le cœur métier de la plateforme LBCFT : le modèle d'évaluation du risque de blanchiment de capitaux et de financement du terrorisme. L'objectif est d'expliquer comment le système identifie, mesure et classe le niveau de risque de chaque client de manière automatisée.

I. IDENTIFICATION ET CLASSIFICATION DES CRITÈRES DE RISQUE

1. Les quatre domaines de risque

La réglementation LBC/FT impose d'évaluer le risque d'un client selon **quatre domaines fondamentaux**. Dans le système, ces domaines sont définis par l'enum *RiskDomainCode* et stockés dans la collection MongoDB *risk_domains* :

Tableau 1 - Tableau représentatif des domaines de risque

Code	Domaine	Ce qu'il évalue
CLIENTS	Risques liés aux Clients	Le profil du client : sa nature (personne physique ou morale), son activité, sa nationalité, s'il est politiquement exposé (PPE)
PRODUITS_SERVICES	Risques liés aux Produits et Services	Les produits financiers utilisés par le client (virements internationaux, crypto-monnaies, comptes anonymes, etc.)
CANAUX	Risques liés aux Canaux de distribution	Le mode de relation avec le client (en face à face, à distance, via un intermédiaire, etc.)
ZONES_GEO	Risques liés aux Zones géographiques	La localisation géographique du client, de ses fournisseurs et de ses opérations (pays à risque, listes noires, paradis fiscaux)

Pourquoi ces 4 domaines ? Ils correspondent aux piliers de l'approche basée sur les risques recommandée par le GAFI (Groupe d'Action Financière) et reprise par les régulateurs nationaux.

2. L'arbre hiérarchique des critères de risque

Le système organise tous les critères de risque sous forme d'un arbre à 4 niveaux. Chaque nœud de cet arbre est un *RiskNode* stocké dans la collection *risk_nodes*. L'arbre est structuré comme suit :

Domaine (CLIENTS, PRODUITS_SERVICES, CANAUX, ZONES_GEO)

- └─ Catégorie (CATEGORY)
 - └─ Facteur (FACTOR)
 - └─ Sous-Facteur (SUB_FACTOR) — optionnel
 - └─ Valeur (VALUE) — porte le score de risque

Les quatre types de nœuds, définis par l'enum *RiskNodeType*, sont :

Tableau 2 - Tableau des types de noeuds

Type	Rôle	Exemple concret
CATEGORY	Regroupe les facteurs d'un même thème	« Type de structure », « Nationalité »
FACTOR	Critère spécifique d'évaluation	
SUB_FACTOR	Sous-division d'un facteur (optionnel)	« Activités à haut risque », « Activités à faible risque »
VALUE	Réponse possible (porte le score de risque (1 à 4))	« Immobilier » (score 3), « Commerce de détail » (score 1)

3. Représentation visuelle de l'arbre de risque

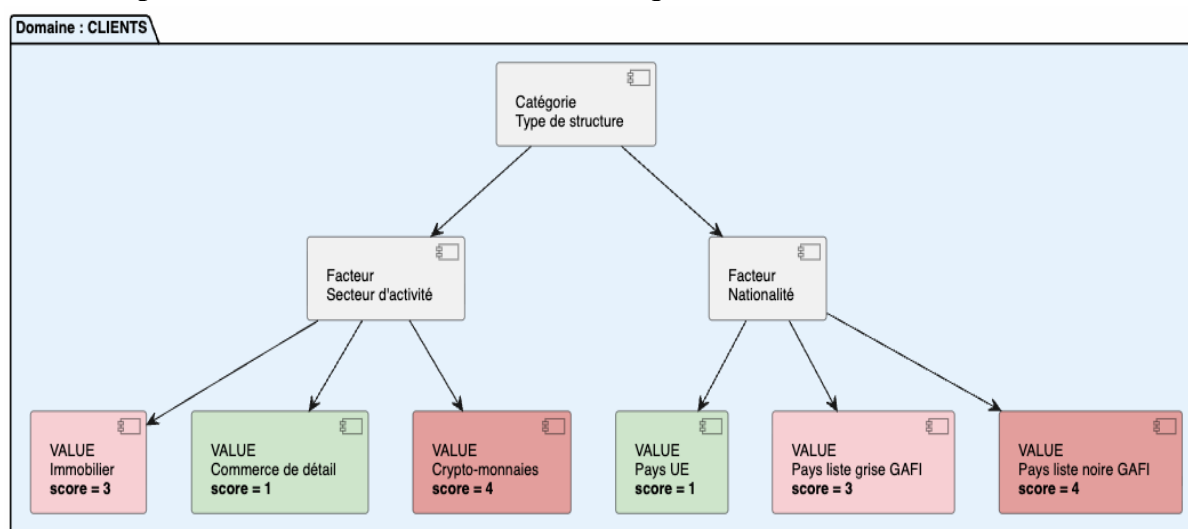


Figure 3 - Arbre Hiérarchique des Critères de Risque: Domaine Clients

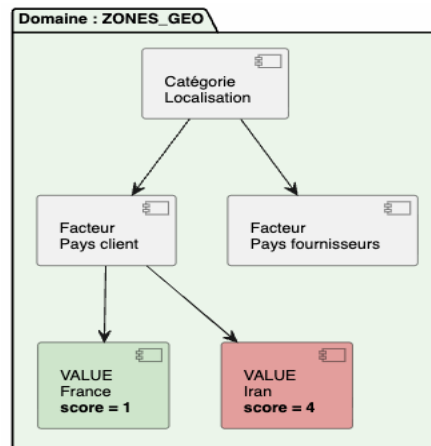


Figure 4 - Arbre Hiérarchique des Critères de Risque Domaine : Zone geo

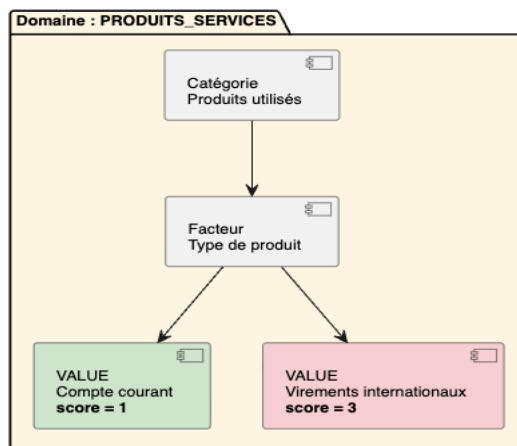


Figure 5 - Arbre Hiérarchique des Critères de Risque Domaine : Produits_ser

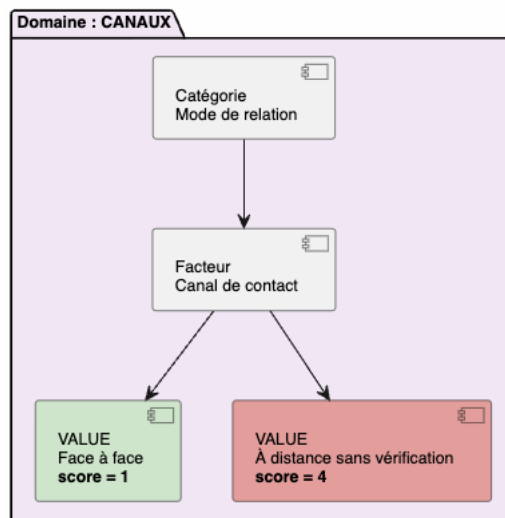


Figure 6 - Arbre Hiérarchique des Critères de Risque Domaine : Canaux

4. Le rôle des facteurs de risque

Les **facteurs de risque** (*RiskFactor*) sont le maillon entre les catégories et les valeurs. Chaque facteur est identifié par :

- Un *factorid* unique ;
- Un *categoryid* qui le rattache à une catégorie ;
- Un *code* et un *label* pour l'identification ;
- Un champ *weight* (poids de pondération, valeur par défaut : 0).

Note importante : Dans l'implémentation actuelle du système, le calcul de risque utilise une moyenne simple (pas de pondération par le *weight*). Le champ *weight* est prévu dans le schéma pour une évolution future vers un calcul pondéré, mais il n'est pas exploité dans la logique de calcul actuelle.

5. Lien entre les critères de risque et le formulaire KYC

Le système utilise un mécanisme de **mapping dynamique** entre les champs du formulaire KYC et les facteurs de risque. Chaque champ du formulaire (*KycFormField*) peut contenir :

- un *factorId*, identifiant du facteur de risque associé ;
- un *nodeSourceId*, identifiant du nœud source pour charger les options dynamiquement ;
- un *categoryId*, identifiant de la catégorie associée.

Ce mapping permet au système de savoir, pour chaque réponse de l'utilisateur, **quel facteur de risque est impacté** et dans **quel domaine** se situe cette réponse.

II. CONSTRUCTION DU MODÈLE DE SCORING DU RISQUE

1. Principe général du scoring

Le modèle de scoring de la plateforme LBCFT repose sur un principe simple mais efficace : chaque réponse au questionnaire KYC porte un score de 1 à 4, qui traduit le niveau de risque associé à cette réponse.

Tableau 3 - Tableau des niveaux de risque

Score	Signification	Couleur dans l'interface
1	Risque Faible	 Vert
2	Risque Moyen	 Jaune
3	Risque Élevé	 Orange
4	Risque Très Élevé	 Rouge

Ce score est défini dans le champ *score* de chaque *RiskNode* de type *VALUE*. Il est fixé lors de la configuration de l'arbre de risque et peut être mis à jour à tout moment par un administrateur.

2. Architecture technique du modèle de scoring

Le modèle de scoring est implémenté dans le service *KycEvaluationsService*, il s'appuie sur les structures de données suivantes.

2.1.La réponse KYC (*KycAnswer*)

Chaque réponse de l'utilisateur est stockée comme un objet avec trois champs :

```
class KycAnswer {
    fieldKey: string;    // Identifiant du champ du formulaire (ex:
    "activity_type")
    nodeId: string;     // ID du RiskNode sélectionné (la valeur choisie)
    score: number;      // Score de risque associé (1 à 4)
}
```

2.2.L'évaluation KYC (*KycEvaluation*)

Le résultat complet d'une évaluation est stocké dans la collection *kyc_evaluations* avec les champs suivants :

Tableau 4 – Tableau de la collection *kyc_evaluations*

Champ	Type	Description
<i>evaluationid</i>	string (UUID)	Identifiant unique de l'évaluation
<i>clientid</i>	string	Le client évalué
<i>cabinetid</i>	string	Le cabinet qui réalise l'évaluation
<i>templateid</i>	string	Le modèle de questionnaire utilisé
<i>answers</i>	KycAnswer[]	Toutes les réponses avec leurs scores
<i>domainScores</i>	Record<string, number>	Score calculé pour chaque domaine
<i>vulnerabilityScore</i>	number	Score de vulnérabilité globale (moyenne des domaines)
<i>menaceScore</i>	number	Score de menace du secteur (1 à 4, saisi par l'évaluateur)
<i>finalScore</i>	number	Résultat final de la matrice de croisement (1 à 4)
<i>finalLabel</i>	RiskLevel	Label de risque (FAIBLE, MOYEN, ELEVE, TRES_ELEVE)
<i>snapshotVersion</i>	number	Version du barème au moment de l'évaluation (pour l'audit)
<i>status</i>	KycStatus	État de l'évaluation (DRAFT, COMPLETED, VALIDATED)

3. Le processus de scoring en 6 étapes

Voici comment le système calcule le risque d'un client, étape par étape :

- **étape 1 — Mapping champ → facteur** : Le système charge le formulaire KYC correspondant au template choisi. Il parcourt tous les champs (*fields*) et construit une table de correspondance : pour chaque clé de champ (*fieldKey*), il enregistre le facteur de risque associé (*factorId*).
- **étape 2 — Traitement des réponses** : Pour chaque réponse de l'utilisateur, le système:
 - Cherche le facteur de risque correspondant via le mapping ;
 - Charge le *RiskNode* sélectionné pour récupérer son *score* et son *domainid* ;
 - Classe le score dans le domaine correspondant.
- **étape 3 — Score par domaine** : Les scores sont regroupés par domaine. Le score de chaque domaine est la **moyenne arithmétique simple** de tous les scores qui lui appartiennent.
- **étape 4 — Vulnérabilité globale** : La vulnérabilité est la **moyenne des scores de tous les domaines** qui ont au moins une réponse.
- **étape 5 — Croisement matriciel** : La vulnérabilité est croisée avec le score de menace du secteur via une matrice 4×4 pour obtenir le score final.
- **étape 6 — Label de risque** : Le score final (1 à 4) est traduit en label textuel.

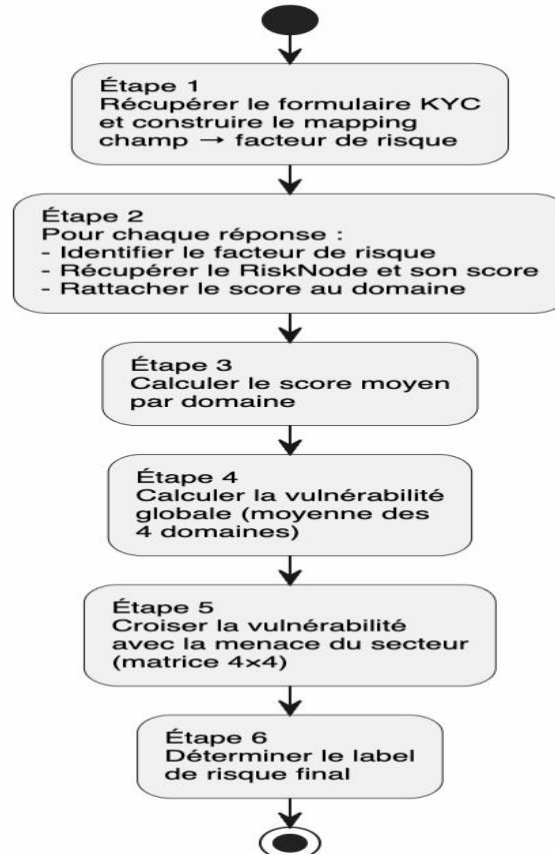


Figure 7 - Processus de Scoring du Risque — Vue d'ensemble

4. Le versioning des évaluations

Un point important du modèle est le champ *snapshotVersion*. Ce champ fige la version du barème de risque au moment de l'évaluation. Si l'administrateur modifie les scores des *RiskNode* par la suite, les évaluations déjà réalisées conservent leur résultat d'origine. Ce mécanisme est essentiel pour l'audit réglementaire : il permet de prouver que l'évaluation a été faite avec le barème en vigueur à la date de l'analyse.

III. APPROCHE MATHÉMATIQUE D'ÉVALUATION DU RISQUE

1. Variables et notations

Posons les notations suivantes :

Tableau 5 - Tableau de symboles

Symbole	Signification
D	L'ensemble des domaines de risque ($D = \{\text{CLIENTS, PRODUITS_SERVICES, CANAUX, ZONES_GEO}\}$)
n	Le nombre de domaines ayant au moins une réponse ($1 \leq n \leq 4$)
d	Un domaine donné ($d \in D$)
F_d	L'ensemble des facteurs évalués dans le domaine d
k_d	Le nombre de facteurs évalués dans le domaine d (k_d)
S_f	Le score du facteur f ($1 \leq S_f \leq 4$, entier)
V_d	Le score de vulnérabilité du domaine d
V_g	Le score de vulnérabilité globale
M	Le score de menace du secteur ($1 \leq M \leq 4$, saisi par l'évaluateur)
R	Le score de risque final ($1 \leq R \leq 4$, entier)

2. Formule de calcul, Score par domaine

Pour chaque domaine d, le score de vulnérabilité est la **moyenne simple** des scores de tous les facteurs évalués dans ce domaine :

$$V_d = \frac{1}{k_d} \sum_{f=1}^{k_d} S_f = \frac{S_1 + S_2 + \dots + S_{k_d}}{k_d}$$

En clair : on additionne les scores de tous les facteurs du domaine et on divise par le nombre de facteurs.

3. Formule de calcul, Vulnérabilité globale

La vulnérabilité globale est la **moyenne des scores de tous les domaines** qui ont au moins une réponse :

$$V_g = \frac{1}{n} \sum_{d=1}^n V_d$$

En clair : on additionne les scores de tous les domaines évalués et on divise par le nombre de domaines.

Pourquoi la moyenne simple et pas la pondération ?

L'approche adoptée est conforme au document « Support Atelier La Fiduciale » (ECA-CI). Elle traite chaque domaine avec le même poids, ce qui reflète le principe réglementaire selon lequel les quatre piliers du risque sont **d'importance égale**.

4. La matrice de croisement Vulnérabilité × Menace

Le score de risque final n'est pas la vulnérabilité seule. Il résulte du croisement entre :

- la vulnérabilité du client (V_d , calculée automatiquement) ;
- la menace du secteur d'activité (M , saisie par l'évaluateur).

Ce croisement se fait via une **matrice 4×4** définie en dur dans le code :

Tableau 6 - Tableau de la matrice de croisement Vulnérabilité × Menace

	V = 1 (Faible)	V = 2 (Moyen)	V = 3 (Élevé)	V = 4 (Très Élevé)
M = 1 (Faible)	1	1	2	3
M = 2 (Moyen)	1	2	3	3
M = 3 (Élevé)	2	3	3	4
M = 4 (Très Élevé)	3	3	4	4

La formule d'accès à la matrice est :

$$R = \text{Matrice}[M][V] \quad \text{avec } M, V \in \{1, 2, 3, 4\}$$

Avant d'accéder à la matrice, la vulnérabilité globale (qui est un nombre décimal) est **arrondie à l'entier le plus proche** et **bornée entre 1 et 4** :

$$V_{\text{arrondi}} = \max(1, \min(4, \text{round}(V_g)))$$

5. Détermination du label de risque final

Le score final R (1 à 4) est traduit en un label textuel défini par l'enum **RiskLevel** :

Tableau 7 - Tableau du label de risque final

Score final (R)	Label	Signification
1	FAIBLE	Le client présente un risque faible de BC/FT

2	MOYEN	Le client présente un risque modéré : vigilance standard
3	ELEVE	Le client présente un risque élevé : vigilance renforcée requise
4	TRES_ELEVE	Le client présente un risque très élevé : mesures de vigilance complémentaires obligatoires

6. Exemple numérique complet

Prenons un cas concret : l'évaluation d'un client fictif « **Société Alpha** » opérant dans le secteur immobilier avec des opérations internationales.

Tableau 8 - Tableau de données d'entrée

Champ du formulaire	Réponse sélectionnée	Domaine	Score
Secteur d'activité	Immobilier	CLIENTS	3
Nationalité	Pays liste grise GAFI	CLIENTS	3
Statut PPE	Non PPE	CLIENTS	1
Produit principal	Virements internationaux	PRODUITS_SERVICES	3
Produit secondaire	Compte courant	PRODUITS_SERVICES	1
Canal de contact	Face à face	CANAUX	1
Pays client	France	ZONES_GEO	1
Pays fournisseur	Iran	ZONES_GEO	4

Score de menace saisi : M = 2 (secteur à menace moyenne)

- **Étape 1 — Scores par domaine**

- **Domaine CLIENTS** : 3 facteurs évalués

$$V_{CLIENTS} = \frac{3 + 3 + 1}{3} = \frac{7}{3} = 2.33$$

- **Domaine PRODUITS_SERVICES** : 2 facteurs évalués

$$V_{PRODUITS} = \frac{3 + 1}{2} = \frac{4}{2} = 2.00$$

- **Domaine CANAUX** : 1 facteur évalué

$$V_{CANAUX} = \frac{1}{1} = 1.00$$

➤ **Domaine ZONES_GEO** : 2 facteurs évalués

$$V_{ZONES} = \frac{1 + 4}{2} = \frac{5}{2} = 2.50$$

- *Étape 2 — Vulnérabilité globale*

4 domaines ont des réponses :

$$V_g = \frac{2.33 + 2.00 + 1.00 + 2.50}{4} = \frac{7.83}{4} = 1.96$$

- *Étape 3 — Arrondi pour la matrice*

$$V_{arrondi} = \text{round}(1.96) = 2$$

- *Étape 4 — Croisement matriciel*

Avec M = 2 (Moyen) et V = 2 (Moyen) :

$$R = \text{Matrice}[2][2] = 2$$

- *Étape 5 — Label final*

$$R = 2 \Rightarrow \text{finalLabel} = \text{MOYEN}$$

Résultat stocké en base :

```
{
  "evaluationid": "a1b2c3d4-...",
  "clientId": "x1y2z3-...",
  "domainScores": {
    "domain-clients-uuid": 2.33,
    "domain-produits-uuid": 2.00,
    "domain-canaux-uuid": 1.00,
    "domain-zones-uuid": 2.50
  },
  "vulnerabilityScore": 1.96,
  "menaceScore": 2,
  "finalScore": 2,
  "finalLabel": "MOYEN",
  "snapshotVersion": 1,
  "status": "COMPLETED"
}
```

7. Diagramme synthétique du modèle mathématique

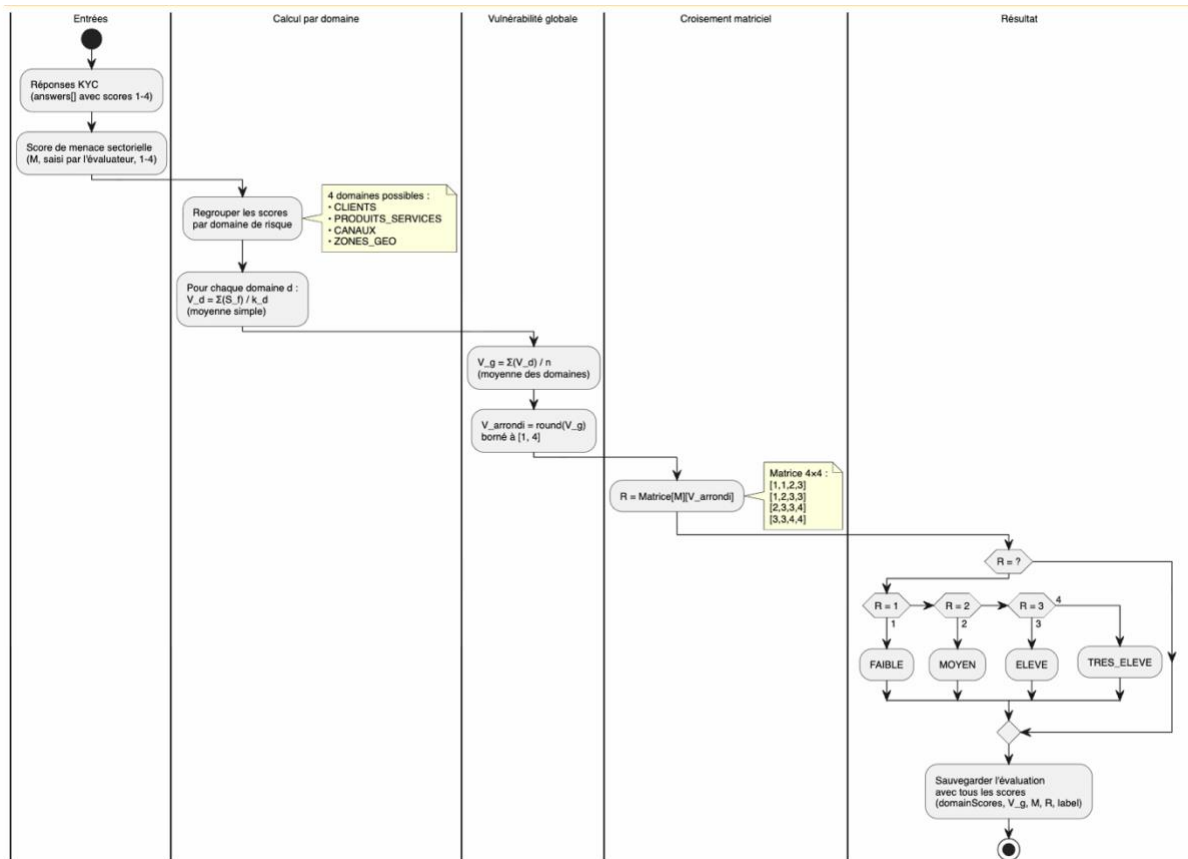


Figure 8 - Modèle Mathématique d'Évaluation du Risque — Synthèse

8. Propriétés mathématiques du modèle

Le modèle d'évaluation possède les propriétés suivantes :

a) Bornes garanties

Puisque chaque score d'entrée $S_i \in \{1, 2, 3, 4\}$, la moyenne par domaine V_d est toujours dans l'intervalle $[1, 4]$. De même, la vulnérabilité globale $V_g \in [1, 4]$. Le résultat final $R \in \{1, 2, 3, 4\}$.

b) Monotonie

Si on augmente le score d'un facteur (en gardant tous les autres inchangés), le score de vulnérabilité ne peut que rester stable ou augmenter. Le modèle ne produit jamais de résultat paradoxal où « plus de risque $\rightarrow$ moins de risque ».

c) Sensibilité à la menace

La matrice est conçue pour que le score final soit **toujours** $\geq \max(M, V) - 1$. Autrement dit, une menace élevée ou une vulnérabilité élevée suffit à tirer le résultat vers le haut. Il n'est pas possible d'avoir simultanément une menace 4 et une vulnérabilité 4 sans obtenir un risque final 4.

d) Symétrie relative

La matrice est presque symétrique ($\text{Matrice}[M][V] \approx \text{Matrice}[V][M]$), ce qui signifie que la menace et la vulnérabilité ont un **poids comparable** dans le résultat final.

e) Principe de prudence

Pour les cas limites ($M = 1, V = 4$ ou $M = 4, V = 1$), la matrice donne un score de 3 (ELEVE) et non de 2.5 arrondi. Cela traduit un **principe de prudence réglementaire** : en cas de doute, le système penche vers le risque le plus élevé.

IV. MÉTHODES STATISTIQUES ET PROBABILISTES POUR L'AMÉLIORATION DU SCORING DE RISQUE

1. Calcul et normalisation du score de risque

L'évaluation actuelle du risque repose sur l'attribution de notes à différents critères de conformité. Ces notes sont ensuite agrégées afin de déterminer le niveau de risque global du client.

Toutefois, avant leur exploitation, les notes peuvent être normalisées afin de les ramener sur une même échelle de valeurs. La normalisation permet d'éviter les écarts liés à des systèmes de notation différents et d'obtenir une évaluation plus homogène.

La formule de normalisation utilisée est la suivante :

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}}$$

Où :

- x représente la valeur observée ;
- $x_{\min}$ représente la valeur minimale possible ;
- $x_{\max}$ représente la valeur maximale possible ;
- x' représente la valeur normalisée.

Dans le contexte de la LBC/FT, cette approche permet d'obtenir un score de risque plus cohérent et plus facilement exploitable pour la classification des clients selon leur niveau de risque.

2. Utilisation de l'entropie pour la détection des comportements atypiques

L'entropie est un concept issu de la théorie de l'information permettant de mesurer le degré d'incertitude ou d'imprévisibilité d'un ensemble de données. Elle est particulièrement utile pour identifier des comportements inhabituels pouvant constituer des indicateurs de risque.

L'entropie de Shannon est définie par la formule suivante :

$$H(X) = - \sum_{i=1}^n P(x_i) \log_2(P(x_i))$$

où :

- x_i représente l'élément observé ;

- $H(X)$ représente l'entropie ;
- $P(x_i)$ représente la probabilité d'apparition d'un événement.

Une faible valeur d'entropie traduit généralement un comportement stable et prévisible, tandis qu'une valeur élevée peut révéler des variations importantes ou des comportements atypiques. Dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme, cette approche pourrait permettre de détecter automatiquement des changements inhabituels dans le comportement d'un client, tels qu'une augmentation soudaine du volume des transactions ou une modification importante des habitudes financières. Cette méthode constitue une perspective d'amélioration de la plateforme et pourrait être intégrée à travers l'entraînement d'un modèle d'intelligence artificielle sur les données historiques.

3. Modèle probabiliste basé sur le théorème de Bayes

Le théorème de Bayes est une méthode statistique permettant d'estimer la probabilité qu'un événement se produise à partir d'informations déjà observées. Il offre une approche plus dynamique de l'évaluation du risque en tenant compte des nouvelles données disponibles.

Sa formulation est la suivante :

$$P(R | D) = \frac{P(D | R) \times P(R)}{P(D)}$$

où :

- $P(R | D)$ représente la probabilité qu'un client soit risqué compte tenu des données observées ;
- $P(D | R)$ représente la probabilité d'observer ces données lorsqu'un client est effectivement risqué ;
- $P(R)$ représente la probabilité initiale de risque ;
- $P(D)$ représente la probabilité d'observer les données.

Dans le cadre de la LBC/FT, cette approche pourrait permettre d'estimer automatiquement la probabilité qu'un client présente un risque élevé à partir d'informations telles que son secteur d'activité, son pays de résidence, son historique de conformité ou la nature de ses transactions.

CHAPITRE V : CONCEPTION DE LA PLATEFORME

La conception d'un système informatique nécessite une approche méthodique et structurée. Ce chapitre présente les méthodes retenues pour la réalisation du projet ainsi que les raisons ayant motivé leur choix.

I. PRÉSENTATION DES MÉTHODES

1. Méthode de modélisation

1.1.Méthode UP

Le **processus unifié (UP)** est une méthode itérative et incrémentale centrée sur l'architecture et les cas d'utilisation. La méthode **UP** est **très structurée**, idéale pour des gros projets complexes mais **lourde** et parfois trop rigide pour des petits projets ou prototypes rapides.

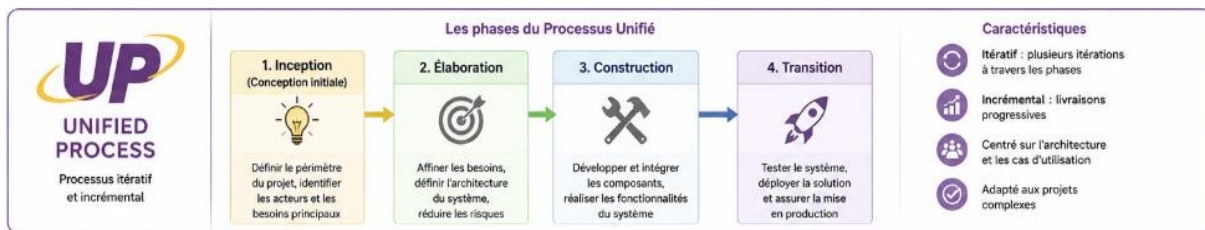


Figure 9 - Illustration du Processus Unifié (UP)

1.1.1 Le langage de modélisation unifié (UML)

UML est un langage de modélisation standard permettant de représenter graphiquement les structures et comportements d'un système.

- Il ne s'agit pas d'une méthode mais d'un langage universel de modélisation.
- Il permet de décrire les aspects statiques et dynamiques du système.

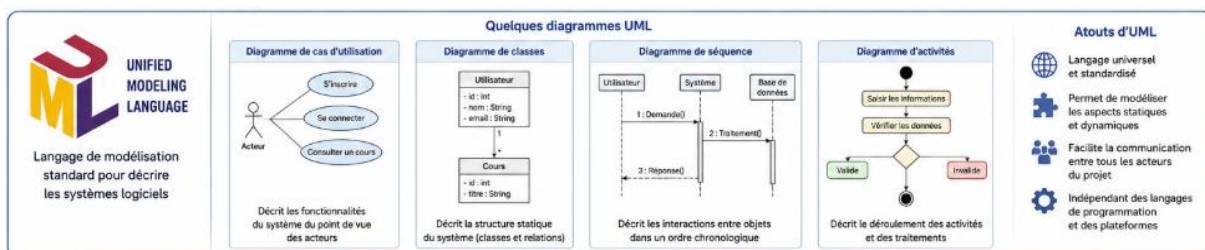


Figure 10 - Illustration du langage UML

1.2.Méthode MERISE

MERISE est une méthode française d'analyse et de conception des systèmes d'information, basée sur la **séparation stricte des données et des traitements**. Elle est largement utilisée pour la modélisation des bases de données relationnelles. **MERISE** est très puissante pour concevoir des **bases de données structurées**, mais elle est aujourd'hui moins utilisée dans les **architectures modernes et agiles**.

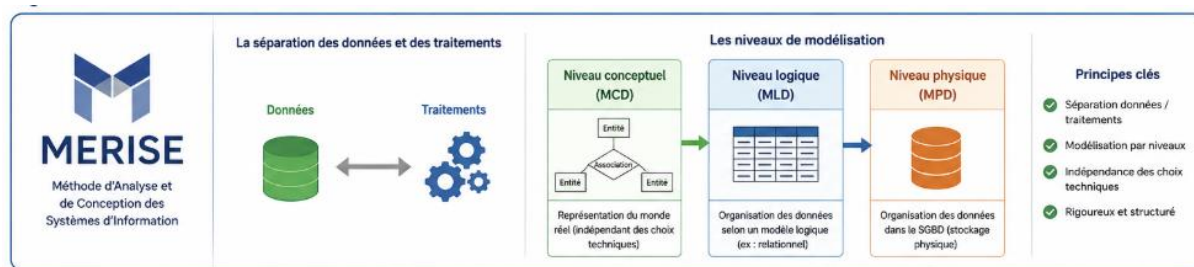


Figure 11 - Illustration de la méthode MERISE

II. ÉTUDE COMPARATIVE ET PRÉSENTATION DES MÉTHODES CHOISIES

1. Étude comparative

1.1.Méthodes de modélisation

Il existe plusieurs méthodes de modélisation, cette étude fera l'objet d'une comparaison entre le langage UML qui utilise la méthode UP et la méthode Merise

Tableau 9 - Tableau comparatif UML - MERISE

Caractéristiques	Méthodes	
	UP	MERISE
Domaine d'application	Modélisation des systèmes logiciels orientés objets	Modélisation des données et des processus métier
Niveau d'abstraction	Plus flexible	Moins flexible
Types de diagrammes	Grande variété de diagramme	Variété de diagramme restreinte
Approche de modélisation	Approche ascendante	Approche descendante
Précision	Tournée vers la réalisation finale car adaptée à n'importe quel langage de POO	Difficultés d'implémentation car éloignée du langage

2. Méthodes choisies

I. Méthode de modélisation

Dans notre quête d'une approche alliant souplesse et rigueur pour atteindre nos objectifs, notre choix s'est porté sur le **Processus Unifié (UP)** pour sa capacité à allier **rigueur et flexibilité**. Cette méthode s'adapte aux évolutions du projet tout en offrant un cadre structuré pour une modélisation efficace. Elle constitue ainsi une approche adaptée pour gérer les exigences et les contraintes de notre développement.

CHAPITRE VI : RÉALISATIONS

I. DIAGRAMME DE CAS D'UTILISATION

Il fournit une vue globale des différentes fonctionnalités et des actions offertes par le système, ce qui aide les concepteurs et les développeurs à comprendre comment le système va être utilisé et comment il répondra aux besoins des utilisateurs. La figure ci-contre présente le diagramme de cas d'utilisation du système.

1. Diagramme de cas d'utilisation

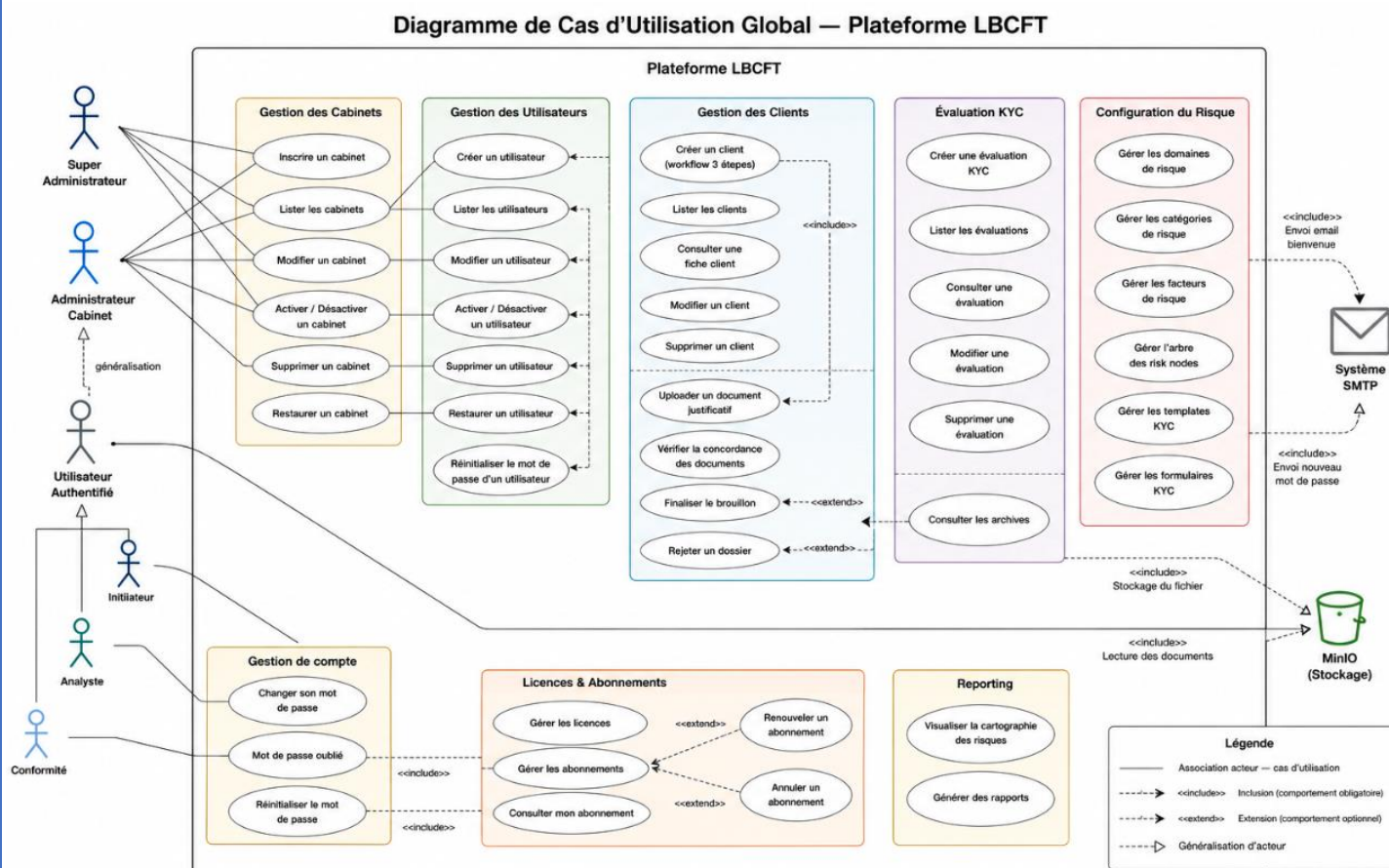


Figure 12 - Diagramme de cas d'utilisation

2. Descriptions textuelles de cas d'utilisation

2.1.Cas d'utilisation « s'authentifier »

Tableau 10 - Cas d'utilisation : s'authentifier

Élément	Description
Nom	Se connecter
Objectif	Authentifier un utilisateur et lui fournir un token JWT
Acteur principal	Tout utilisateur (superadmin, admin, initiateur, analyste, conformité)
Préconditions	L'utilisateur possède un compte actif avec email et mot de passe
Scénario nominal	1. L'utilisateur saisit email et mot de passe 2. Le système vérifie l'existence dans <i>accés</i> 3. Le système vérifie <i>isactive</i> dans <i>utilisateurs</i> 4. Le système compare le hash bcrypt 5. Le système génère un couple access/refresh token 6. Le refresh token hashé est stocké en base 7. La date de dernière connexion est mise à jour 8. Le système retourne les tokens et le profil utilisateur
Scénarios alternatifs	3a. Email inexistant → 401 "Email ou mot de passe incorrect". 3b. Utilisateur désactivé → 401 "Utilisateur désactivé". 4a. Mot de passe incorrect → 401 "Email ou mot de passe incorrect"
Postconditions	Un JWT valide est disponible côté client pour les requêtes authentifiées

Tableau 11 - Cas d'utilisation : Créer un client (workflow à 3 étapes)

Élément	Description
Nom	Créer un client (workflow 3 étapes)
Objectif	Créer une fiche client complète avec documents justificatifs et vérification
Acteur principal	Initiateur
Préconditions	L'utilisateur est authentifié, son cabinet a un abonnement actif

Scénario nominal	Étape 1 : L'initiateur saisit les informations du client (PP ou PM) et les données de formulaire KYC → Un brouillon est créé (<i>client_drafts</i>). Étape 2 : L'initiateur uploades les documents justificatifs (PDF, images) → Les fichiers sont stockés dans MinIO, les métadonnées dans le brouillon. Étape 3 : L'analyste vérifie la concordance de chaque document (approved/rejected) → Le brouillon est finalisé : un client réel est créé (<i>clients</i>), une archive KYC est générée (<i>kyc_archives</i>), et le brouillon passe au statut FINALIZED
Scénarios alternatifs	3a. Document non conforme → L'analyste rejette le dossier avec un motif, le brouillon retourne à l'étape précédente avec l'historique de rejet
Postconditions	Un client réel existe dans la collection <i>clients</i> , une archive KYC est créée pour l'audit

Tableau 12 - Cas d'utilisation : Créer une évaluation KYC

Élément	Description
Nom	Créer une évaluation KYC
Objectif	Évaluer le niveau de risque LBC/FT d'un client
Acteur principal	Initiateur, Admin, Analyste
Préconditions	Le client existe, un template et un formulaire KYC sont configurés, l'abonnement est actif
Scénario nominal	1. L'utilisateur sélectionne un client et un template KYC 2. Le système charge le formulaire KYC dynamique 3. L'utilisateur répond aux questions (sélection de risk nodes) 4. Le système calcule les scores par domaine (moyenne simple des facteurs) 5. Le système calcule la vulnérabilité globale (moyenne des domaines) 6. Le système croise avec la menace du secteur via la matrice 4×4 7. Le système détermine le label de risque final 8. L'évaluation est sauvegardée
Scénarios alternatifs	4a. Aucune réponse fournie → Scores par défaut (1 = FAIBLE). 6a. Score vulnérabilité ou menace hors limites → Borné à [1, 4]
Postconditions	L'évaluation est créée avec un <i>finalScore</i> et un <i>finalLabel</i> (FAIBLE, MOYEN, ELEVE, TRES_ELEVE)

II. DIAGRAMMES (SÉQUENCE, ACTIVITÉ, CLASSE)

1. Diagrammes de séquence

Le diagramme de séquence est utilisé pour illustrer de manière chronologique les interactions entre les différents objets et acteurs du système. Les interactions entre les éléments du système sont généralement représentées par des flux de messages.

1.1. Diagramme de Séquence, Authentification (Login)

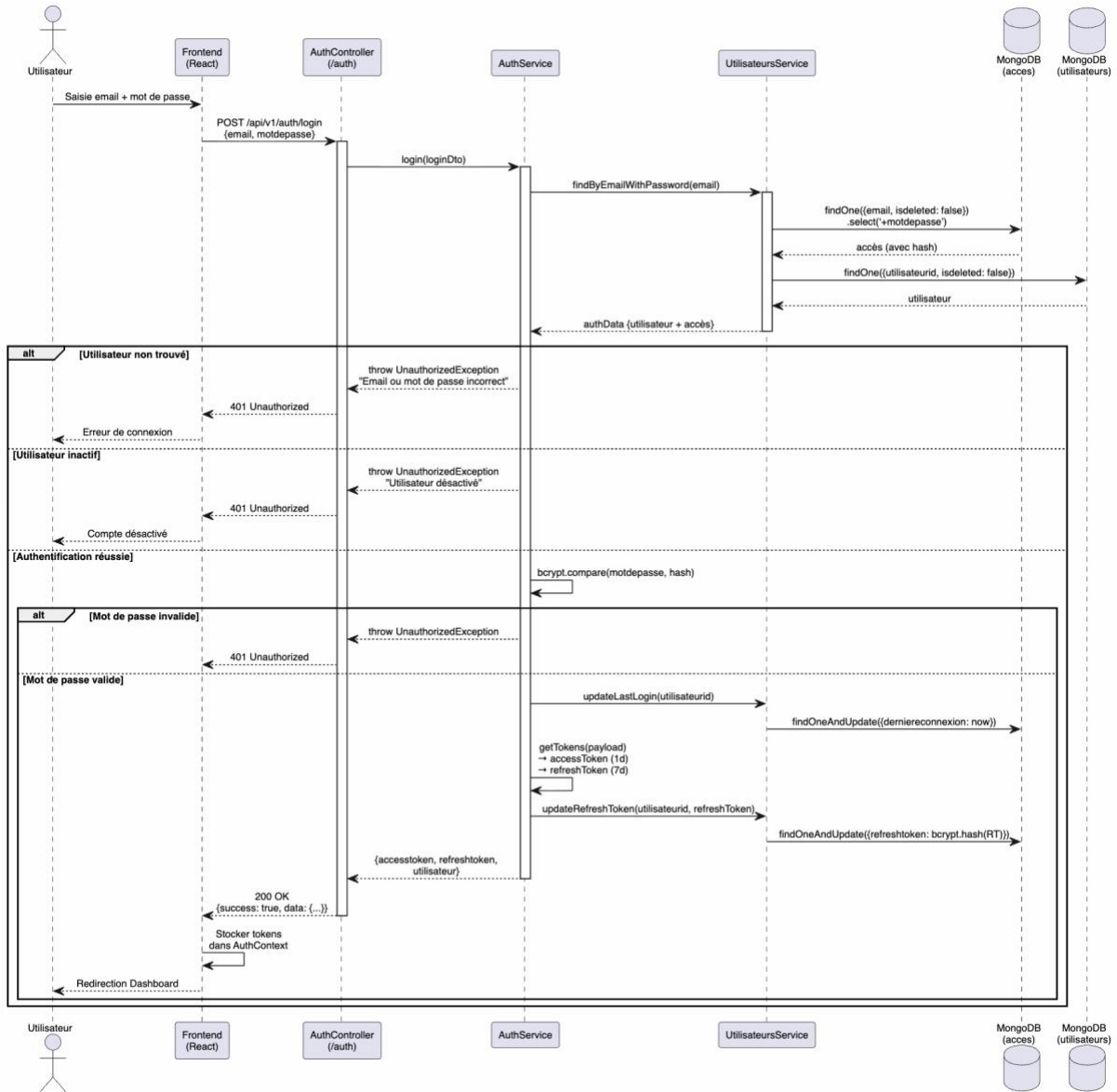


Figure 13 - Diagramme de Séquence, Authentification (Login)

1.2. Diagramme de Séquence, Création d'un Utilisateur

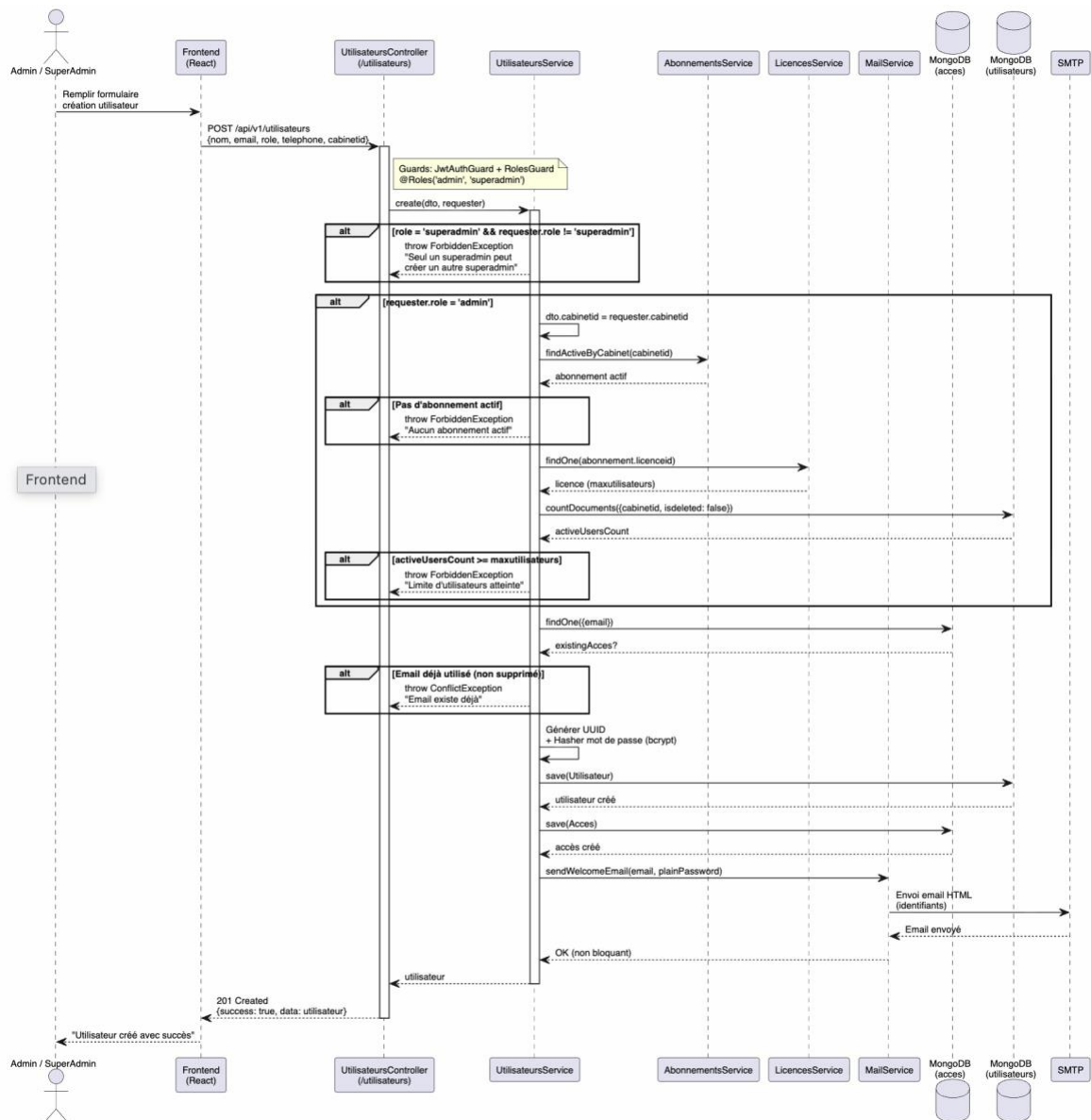


Figure 14 - Diagramme de Séquence, Création d'un Utilisateur

1.3. Diagramme de Séquence, Évaluation KYC avec Calcul de Risque

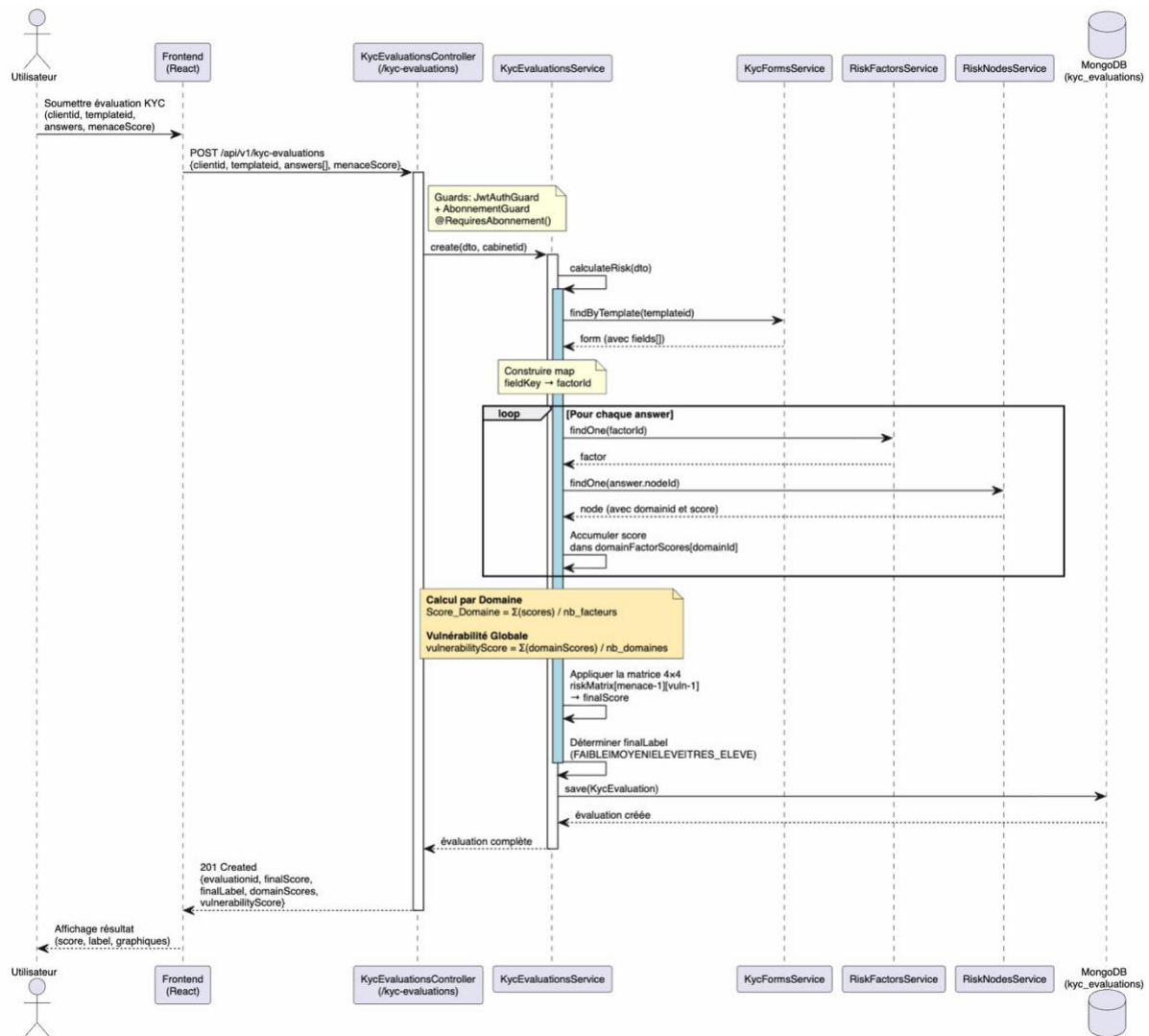


Figure 15 - Diagramme de Séquence, Évaluation KYC avec Calcul de Risque

1.4. Diagramme de Séquence, Mot de Passe Oublié

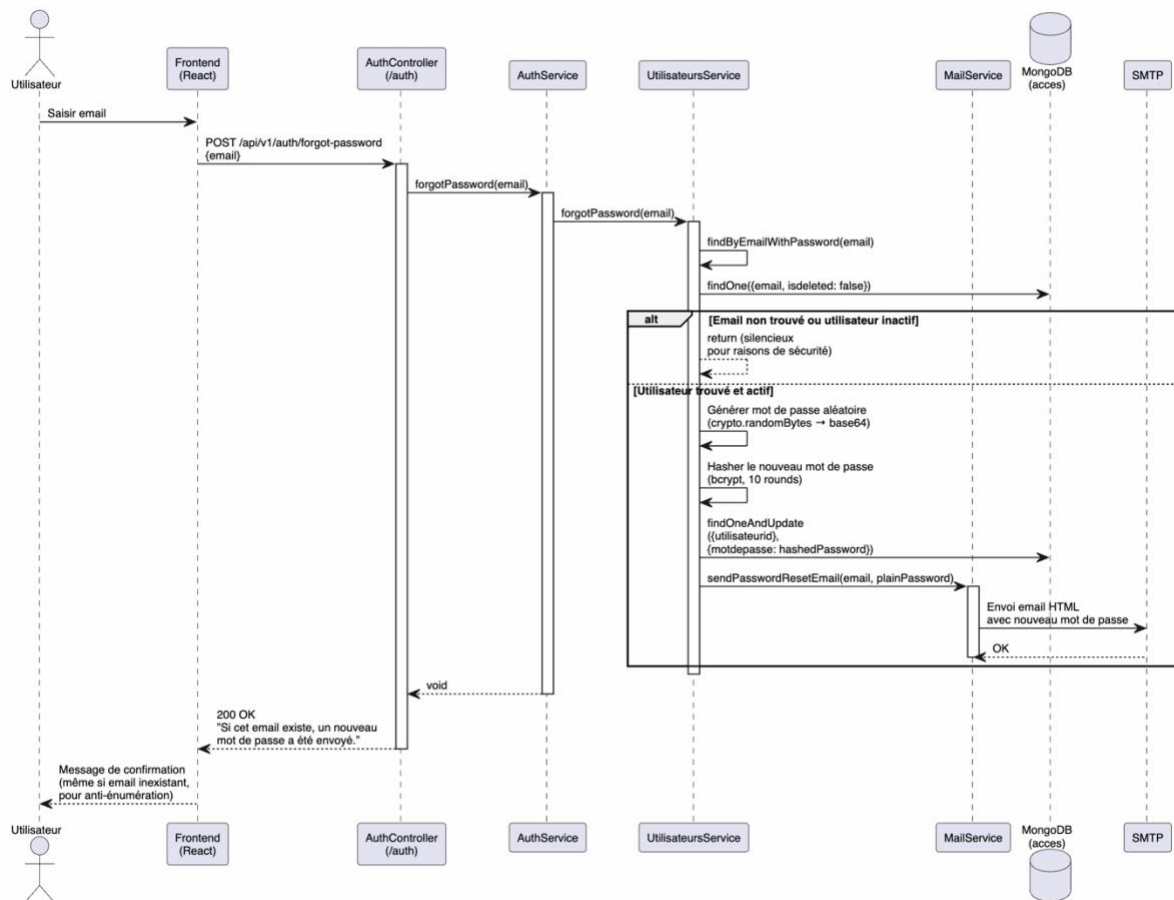


Figure 16 - Diagramme de Séquence, Mot de Passe Oublié

2. Diagrammes d'activité

Le diagramme d'activité est utilisé pour représenter de manière séquentielle le déroulement d'un processus métier ou d'un cas d'utilisation. Il met en évidence les différentes activités, les décisions, les conditions et les flux de contrôle permettant de décrire le comportement dynamique du système.

I. Diagrammes d'activité, Processus d'Authentification

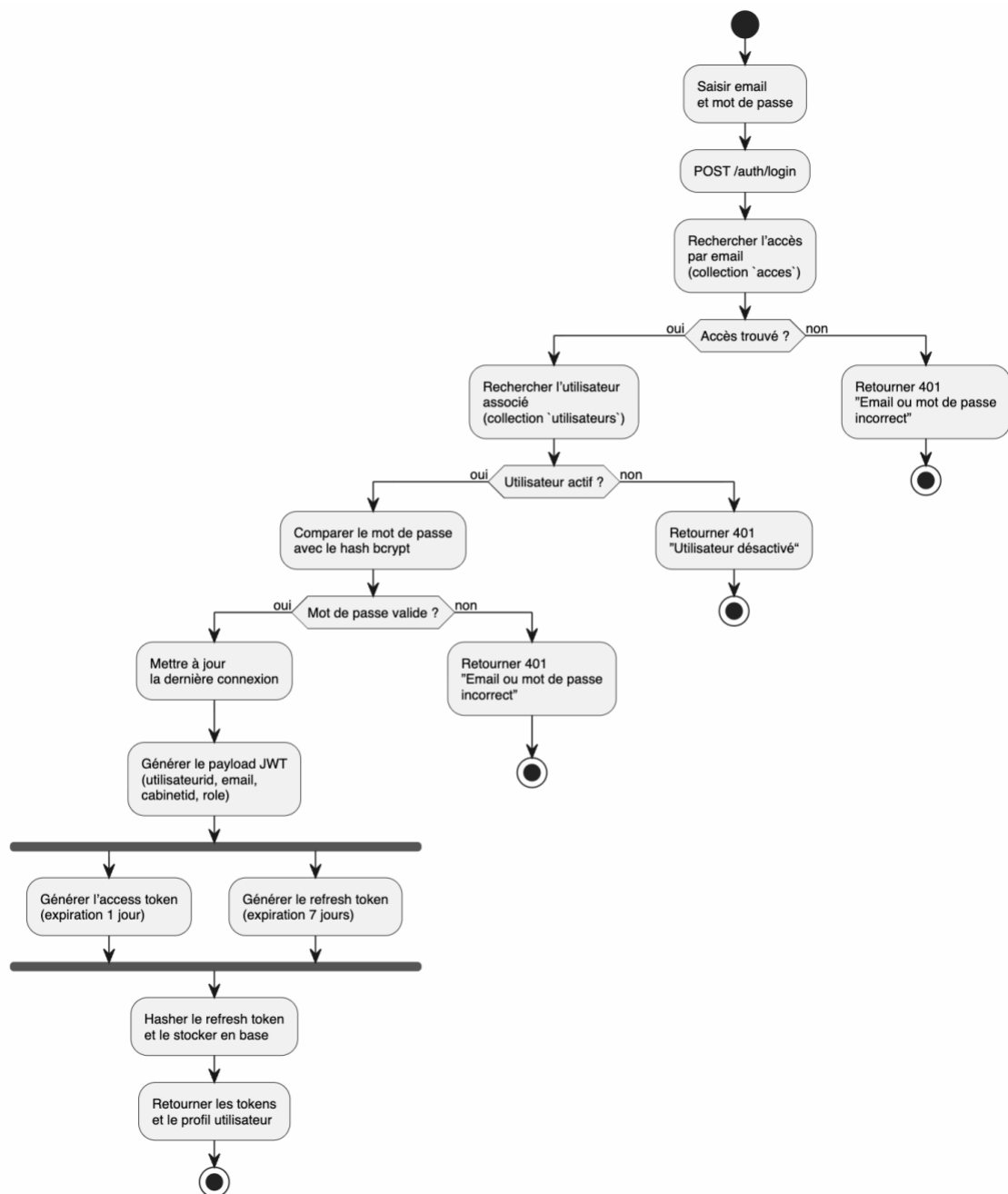


Figure 17 - Diagramme d'activité, Processus d'Authentification

II. Diagramme d'Activité, Création de Client (Workflow 3 Étapes)

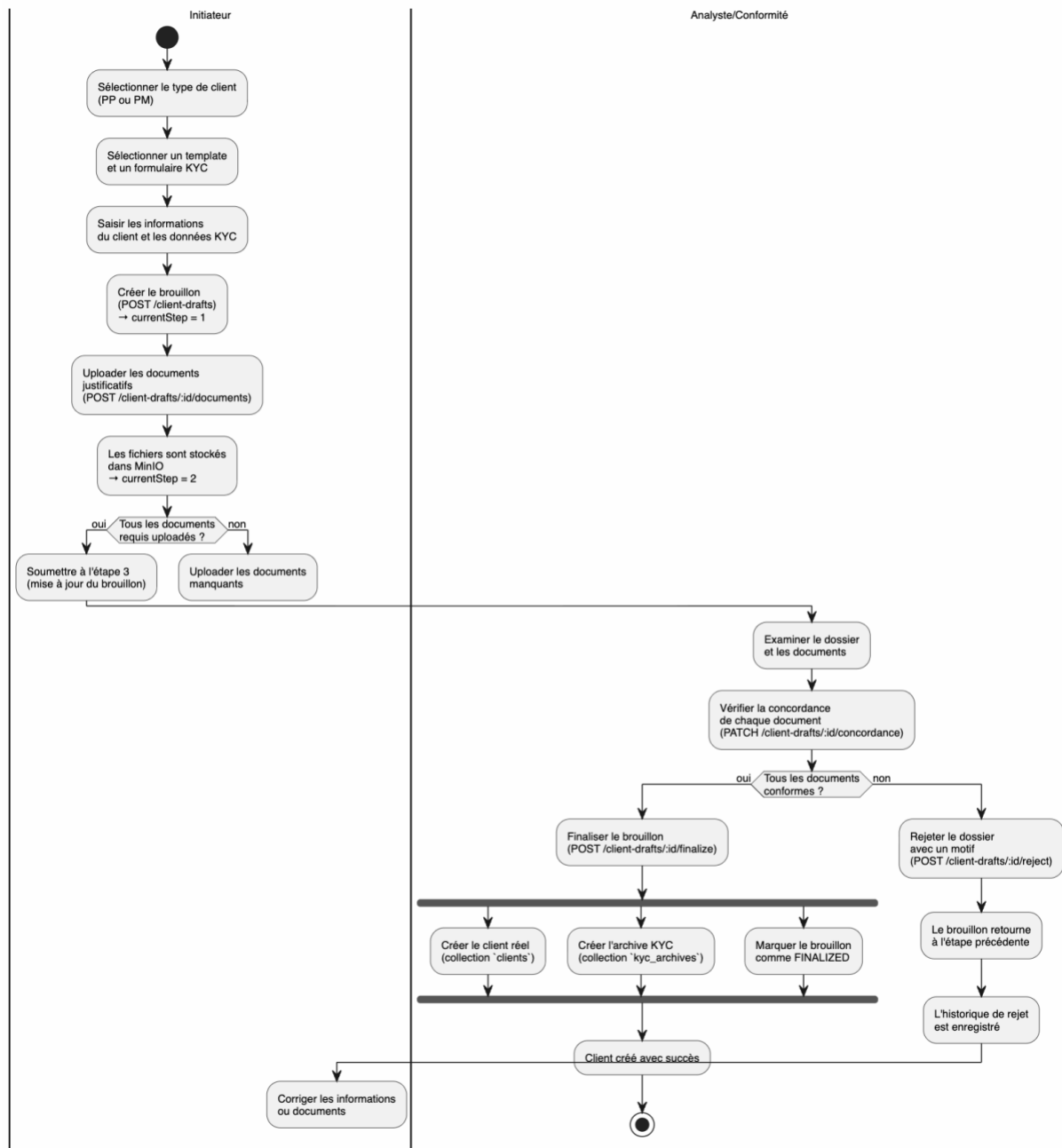


Figure 18 - Diagramme d'Activité, Création de Client (Workflow 3 Étapes)

3. Diagrammes de classes

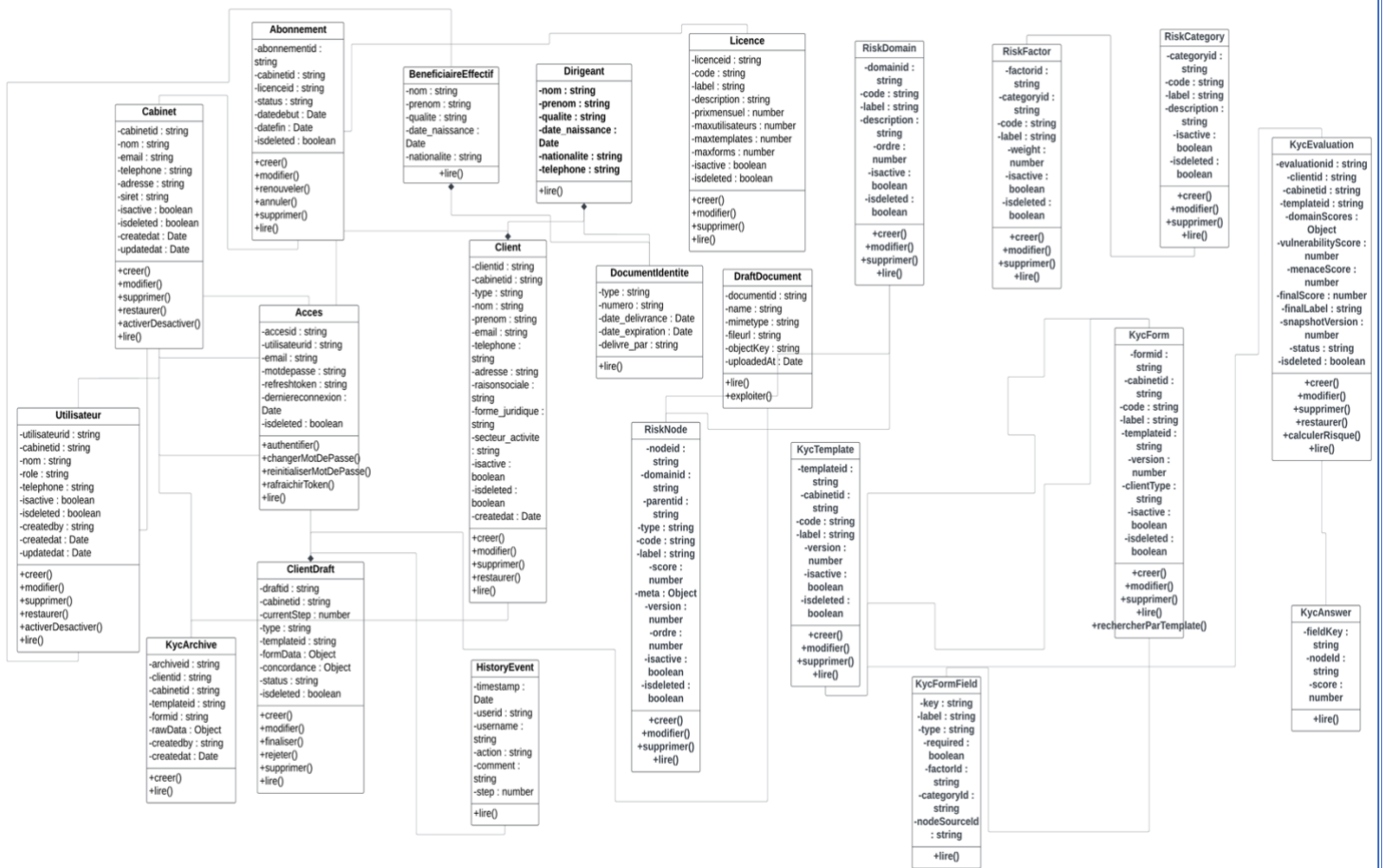


Figure 19 - Diagramme de classes

TROISIÈME PARTIE : RÉSULTATS ET DISCUSSIONS

Cette partie présente les résultats obtenus après et la discussion de ses résultats.

CHAPITRE VII : RÉSULTATS

Ce chapitre offre un aperçu des outils utilisés dans la mise en place du projet et présente les résultats obtenus.

I. OUTILS ET TECHNOLOGIES UTILISÉS

1. Outils et technologies utilisés

1.1.JavaScript

JavaScript est un langage de programmation polyvalent et dynamique, créé en 1995 par Brendan Eich. Initialement conçu pour ajouter de l'interactivité aux pages web, il est devenu l'un des piliers du développement web moderne. JavaScript s'exécute côté client dans les navigateurs web, mais aussi côté serveur grâce à des environnements comme Node.js. Il permet de manipuler le contenu des pages web, de réagir aux actions des utilisateurs, et de communiquer avec des serveurs sans recharger la page. JavaScript est un langage à typage dynamique et à objets, supportant les paradigmes de programmation fonctionnelle et orientée objet. Il est constamment amélioré, avec des mises à jour régulières apportant de nouvelles fonctionnalités. Grâce à sa flexibilité et à son écosystème riche en bibliothèques et frameworks (comme React, Angular, ou Vue.js), JavaScript est utilisé pour développer une grande variété d'applications, des sites web interactifs aux applications mobiles et de bureau.

1.2.ReactJs

ReactJs est une librairie JavaScript permettant de simplifier la création d'interface utilisateur. C'est une technologie qui permet notamment de créer des sites internet sous forme de Single Page Application (des sites internet qui sont constitués d'une seule page). Cette technologie nous a permis de créer notre application web rapides et maintenables.

1.3.TypeScript

TypeScript est un langage de programmation développé par Microsoft qui étend JavaScript en y ajoutant le typage statique et des fonctionnalités avancées orientées objet. Il permet de détecter de nombreuses erreurs dès la phase de développement, améliorant ainsi la qualité, la maintenabilité et la robustesse du code. Cette technologie nous a permis de développer une application plus fiable, mieux structurée et plus facile à maintenir.

1.4.NestJs

NestJS est un framework Node.js basé sur TypeScript permettant de simplifier le développement d'applications backend. Grâce à son architecture modulaire et à ses nombreuses fonctionnalités intégrées, il facilite la création d'API performantes, sécurisées et maintenables. Cette technologie nous a permis de développer un backend robuste et évolutif pour notre application.

1.5.MongoDB Compass

MongoDB Compass est l'interface graphique officielle de MongoDB permettant d'explorer, d'analyser et d'administrer les bases de données MongoDB. Il offre des fonctionnalités de visualisation des données, d'exécution de requêtes et de suivi des performances. Cet outil nous a permis de faciliter la gestion, l'inspection et le contrôle des données stockées dans notre base de données.

1.6.1Panel

1Panel est une plateforme open source d'administration de serveurs offrant une interface web intuitive pour la gestion des applications, des conteneurs, des bases de données et des services système. Elle simplifie les opérations de déploiement, de supervision et de maintenance de l'infrastructure. Cet outil nous a permis d'administrer efficacement nos serveurs et de centraliser la gestion des différents composants de notre environnement.

1.7.MinIO

MinIO est une solution de stockage d'objets compatible avec l'API Amazon S3, conçue pour stocker et gérer de grands volumes de fichiers de manière sécurisée et performante. Elle permet le stockage de documents, d'images et d'autres ressources numériques au sein d'une infrastructure distribuée. Cette technologie nous a permis d'assurer une gestion fiable et évolutive des fichiers utilisés par notre application.

1.8.GitHub

GitHub est une plateforme de gestion de versions basée sur Git qui permet d'héberger, de suivre et de collaborer sur des projets logiciels. Elle offre des fonctionnalités de gestion du code source, de suivi des modifications et de collaboration entre développeurs. Cette plateforme nous a permis de centraliser le code du projet, de faciliter le travail collaboratif et d'assurer le suivi des différentes versions de l'application.

1.9.Jenkins

Jenkins est un outil d'intégration et de déploiement continu (CI/CD) permettant d'automatiser les processus de compilation, de test et de déploiement des applications. Il contribue à améliorer la qualité du logiciel et à accélérer les cycles de développement. Cette technologie nous a permis d'automatiser les déploiements et de garantir une livraison plus rapide et plus fiable des différentes versions de notre application.

1.10. CSS

CSS (Cascading Style Sheets) est un langage utilisé pour décrire l'apparence et la mise en forme des documents HTML. Il permet de contrôler l'agencement, les couleurs, les polices, les espacements, et d'autres aspects visuels des pages web. CSS permet de séparer le contenu

(HTML) de la présentation, ce qui facilite la maintenance et la mise à jour des styles. Il prend également en charge les designs réactifs, permettant aux sites web de s'adapter à différentes tailles d'écran.

1.11. Tailwind CSS

Tailwind CSS est un framework CSS utilitaire permettant de concevoir rapidement des interfaces utilisateur modernes et personnalisées. Grâce à son approche basée sur des classes utilitaires prédéfinies, il facilite le développement d'interfaces cohérentes, responsives et maintenables. Cette technologie nous a permis de créer une interface utilisateur attractive tout en réduisant le temps de développement et de maintenance du style de l'application.

2. Environnement de développement

2.1. Visual Studio Code

VS Code est un éditeur de code multi-plateforme Microsoft. Supporte nombreux langages. Utilisé pour développer applications, API et serveurs d'API.

2.2. MongoDB

MongoDB est un système de gestion de base de données **NoSQL** orienté documents permettant de stocker et de manipuler des données sous format JSON. Grâce à sa flexibilité et à sa capacité à gérer de grands volumes de données, il constitue une solution adaptée aux applications modernes nécessitant une forte évolutivité. Cette technologie nous a permis de stocker efficacement les données de notre application tout en garantissant de bonnes performances et une grande flexibilité dans la gestion des informations.

3. Matériel utilisé

Le matériel utilisé, ainsi que ses caractéristiques techniques pour la réalisation du projet, sont présentés dans le tableau ci-dessous :

Tableau 13 - Tableau récapitulatif du matériel utilisé

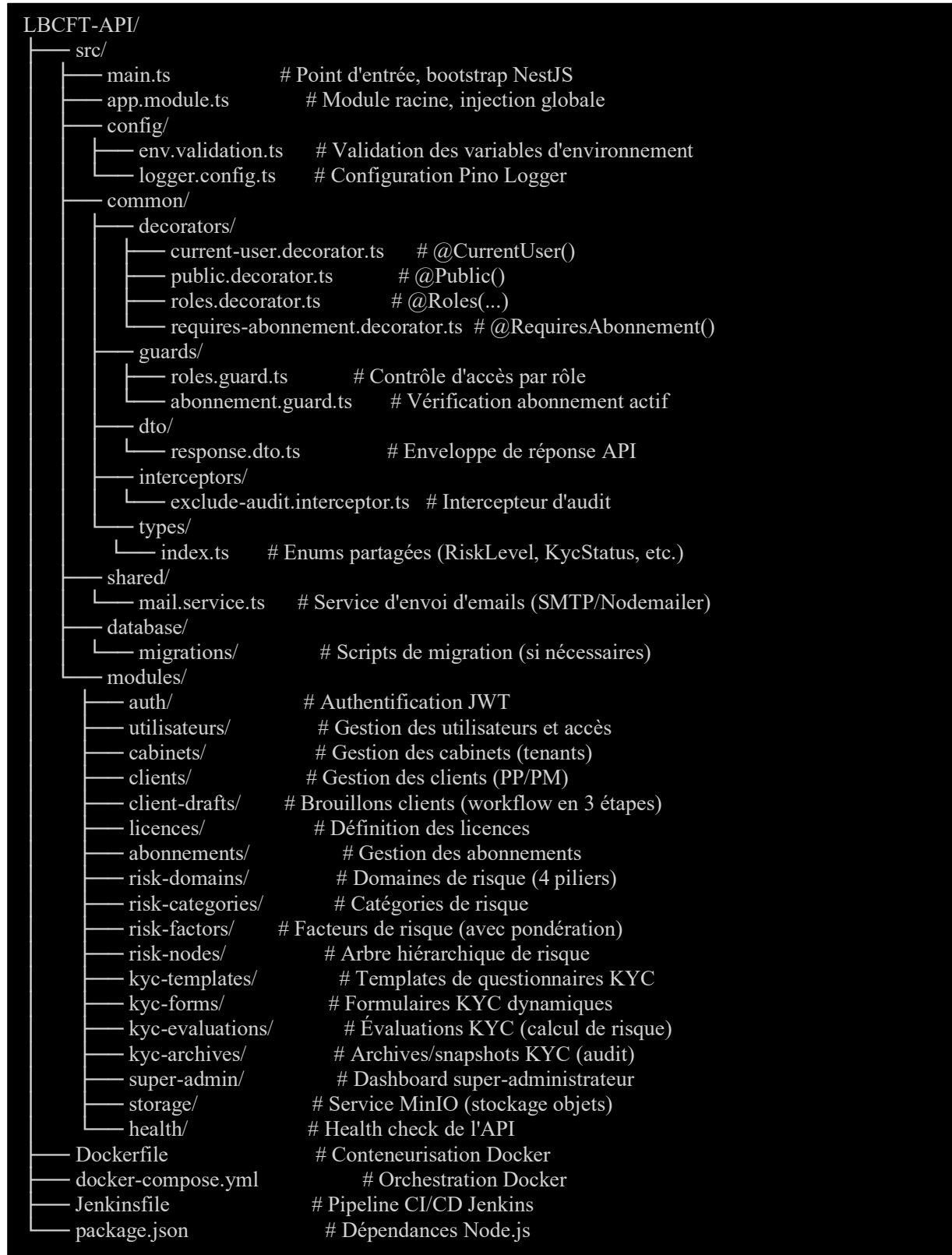
Caractéristiques	Ordinateur
Système d'exploitation	macOS Sequoia 15.6
Processus CPU	Puce Apple M4
Mémoire morte	2 Téra Octets
Mémoire vive (RAM)	16 Gigas octets
Marque	Apple iMac mini (2024)

II. PRÉSENTATION DES RÉSULTATS

1. Présentation de la structure du projet « LBCFT »

1.1.Arborescence du Projet

Backend (LBCFT-API) - NestJS



Frontend (lbcft-site-web) - React + Vite + TailwindCSS

```

lbcft-site-web/
├── src/
│   ├── App.tsx           # Routeur principal React
│   ├── main.tsx          # Point d'entrée Vite
│   └── pages/
│       ├── Login.tsx      # Connexion
│       ├── Register.tsx   # Inscription cabinet
│       ├── ForgotPassword.tsx # Mot de passe oublié
│       ├── Dashboard.tsx  # Tableau de bord
│       ├── Clients.tsx / ClientNew.tsx / ClientDetail.tsx / ClientEdit.tsx
│       ├── Evaluations.tsx / NewEvaluation.tsx / EvaluationDetail.tsx
│       ├── DocumentReview.tsx # Revue de documents (concordance)
│       ├── RiskMap.tsx     # Cartographie des risques
│       ├── Reports.tsx     # Rapports
│       ├── Archives.tsx   # Archives KYC
│       ├── Profile.tsx    # Profil utilisateur
│       ├── admin/         # Pages Admin (Users, Cabinets, MySubscription)
│       ├── super-admin/   # Pages Super Admin (Dashboard, Cabinets, Licenses, Subscriptions, Users)
│       ├── client-portal/ # Portail client (MyProfile, MyDocuments, MyEvaluations, MyHistory)
│       └── data/          # Gestion données de référence (RiskDomains, RiskNodes, etc.)
│   ├── services/         # Couche d'appel API
│   ├── contexts/         # Contexte d'authentification React
│   ├── components/       # Composants réutilisables UI
│   ├── types/            # Types TypeScript
│   ├── hooks/            # Hooks personnalisés
│   ├── schemas/          # Schémas de validation (Zod)
│   └── store/            # Gestion d'état
├── tailwind.config.ts    # Configuration TailwindCSS
├── vite.config.ts        # Configuration Vite
└── package.json          # Dépendances frontend
    
```

1.2.Fonctionnalités de l'application web

Tableau 14 - Tableau des modules fonctionnels

#	Module	Description	Collection MongoDB
1	Auth	Authentification JWT (login, refresh, me, forgot-password)	<i>acces</i>
2	Utilisateurs	Gestion des comptes (CRUD, activation, soft delete, mots de passe)	<i>utilisateurs, acces</i>

3	Cabinets	Gestion des entités organisationnelles (multi-tenancy)	<i>cabinets</i>
4	Clients	Fiches clients Personnes Physiques (PP) et Morales (PM)	<i>clients</i>
5	Client Drafts	Workflow en 3 étapes : saisie → documents → concordance/finalisation	<i>client_drafts</i>
6	Licences	Définition des plans (Standard, Premium, Enterprise)	<i>licences</i>
7	Abonnements	Souscriptions des cabinets aux licences	<i>abonnements</i>
8	Risk Domains	4 domaines réglementaires (Clients, Produits/Services, Canaux, Zones Géo)	<i>risk_domains</i>
9	Risk Categories	Catégories de risque sous chaque domaine	<i>risk_categories</i>
10	Risk Factors	Facteurs de risque pondérés	<i>risk_factors</i>
11	Risk Nodes	Arbre hiérarchique : Category → Factor → Sub-Factor → Value	<i>risk_nodes</i>
12	KYC Templates	Modèles de questionnaires KYC	<i>kyc_templates</i>
13	KYC Forms	Structure dynamique des formulaires (champs, validations, layout)	<i>kyc_forms</i>
14	KYC Evaluations	Résultats d'évaluation avec calcul automatique de risque	<i>kyc_evaluations</i>
15	KYC Archives	Snapshots immuables pour audit réglementaire	<i>kyc_archives</i>
16	Storage	Service MinIO pour le stockage de documents (justificatifs)	X
17	Super Admin	Dashboard statistique global (cabinets, utilisateurs, licences)	X
18	Health	Endpoint de vérification de santé de l'API	X

1.3. Acteurs du Système

Tableau 15 - Tableau des acteurs du système

Acteur	Rôle dans le code (role)	Description
Super Administrateur	<i>superadmin</i>	Gestion globale de la plateforme : cabinets, licences, abonnements, tous les utilisateurs. Bypass des restrictions d'abonnement.

Administrateur de Cabinet	<i>admin</i>	Gestionnaire d'un cabinet spécifique. Crée des utilisateurs, gère les clients et les évaluations KYC de son cabinet. Soumis aux limites de licence.
Initiateur	<i>initiateur</i>	Utilisateur opérationnel qui saisit les fiches clients, lance les brouillons et prépare les dossiers KYC.
Analyste	<i>analyste</i>	Utilisateur chargé d'analyser les évaluations de risque et de valider les résultats.
Conformité	<i>conformite</i>	Responsable de la conformité réglementaire, revue et validation finale des dossiers.
Système SMTP	-	Service externe d'envoi d'emails (bienvenue, réinitialisation de mot de passe).
MinIO (Stockage)	-	Service de stockage objet compatible S3 pour les documents justificatifs.

1.4.Mécanismes d'Authentification et Sécurité

L'authentification repose sur une architecture **JWT (JSON Web Token)** avec rotation de tokens :

- **Stratégie Passport JWT** : Extraction du token depuis le header *Authorization: Bearer <token>*.
- **Guard global** : *JwtAuthGuard* appliqué à toutes les routes (via *APP_GUARD*). Les routes publiques sont marquées par le décorateur *@Public()*.
- **Contrôle d'accès par rôle** : *RolesGuard* avec le décorateur *@Roles('admin', 'superadmin')*.
- **Guard d'abonnement** : *AbonnementGuard* avec *@RequiresAbonnement()* vérifie qu'un abonnement actif et non expiré existe pour le cabinet de l'utilisateur.
- **Rate limiting** : *ThrottlerGuard* (60 requêtes par minute par défaut).
- **Sécurité HTTP** : Helmet (headers de sécurité), CORS activé, validation globale des DTOs (*whitelist, forbidNonWhitelisted*).
- **Hachage des mots de passe** : bcrypt (10 rounds).
- **Refresh token** : Stocké hashé en base, rotation à chaque rafraîchissement.
- **Séparation Utilisateur/Accès** : Les identifiants de connexion (email, mot de passe, refresh token) sont dans la collection *acces*, séparée de la collection *utilisateurs*. Cela renforce la sécurité par ségrégation des données sensibles.

1.5.Flux de Données Principaux

- **Flux 1 : Inscription d'un cabinet**

```
Navigateur → POST /cabinets → CabinetsService.create()
→ Création Cabinet (MongoDB `cabinets`)
→ Création Utilisateur Admin (MongoDB `utilisateurs`)
→ Création Accès avec mot de passe hashé (MongoDB `acces`)
→ Envoi email de bienvenue (SMTP via MailService)
```

- **Flux 2 : Évaluation KYC d'un client**

```
Utilisateur → POST /kyc-evaluations → KycEvaluationsService.create()
→ Récupération du formulaire (KycFormsService.findByTemplate())
→ Pour chaque réponse :
→ Récupération du facteur de risque (RiskFactorsService)
→ Récupération du noeud de risque et score (RiskNodesService)
→ Calcul score par domaine (moyenne simple)
→ Calcul vulnérabilité globale (moyenne des domaines)
→ Croisement matrice Vulnérabilité × Menace → Score final (1-4)
→ Détermination du label (FAIBLE, MOYEN, ELEVE, TRES_ELEVE)
→ Sauvegarde évaluation (MongoDB `kyc_evaluations`)
```

- **Flux 3 : Workflow de création client (3 étapes)**

```
Étape 1 : POST /client-drafts (saisie informations → formData)
Étape 2 : POST /client-drafts/:id/documents (upload justificatifs → MinIO)
Étape 3 : PATCH /client-drafts/:id/concordance (vérification documents)
→ POST /client-drafts/:id/finalize (création client réel + archive KYC)
→ POST /client-drafts/:id/reject (retour étape précédente si non conforme)
```

2. Description en image de l'application web



Figure 20 - Landing page

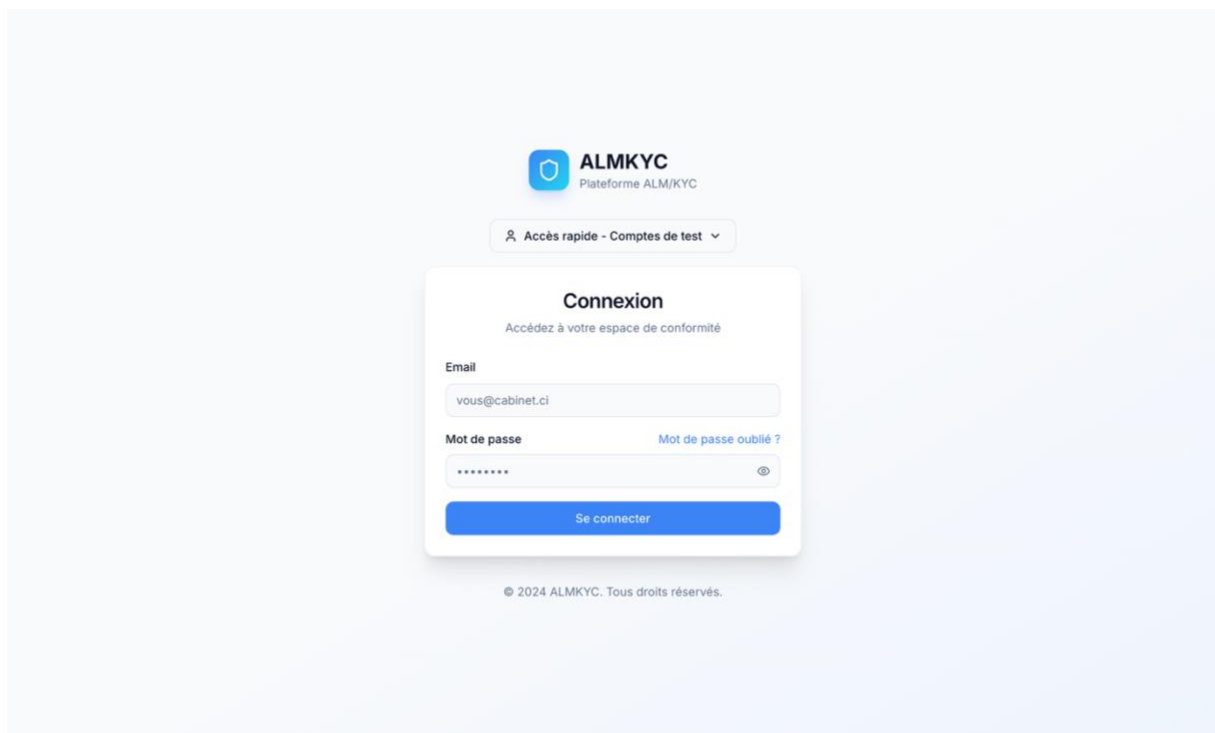


Figure 21 - Page d'authentification

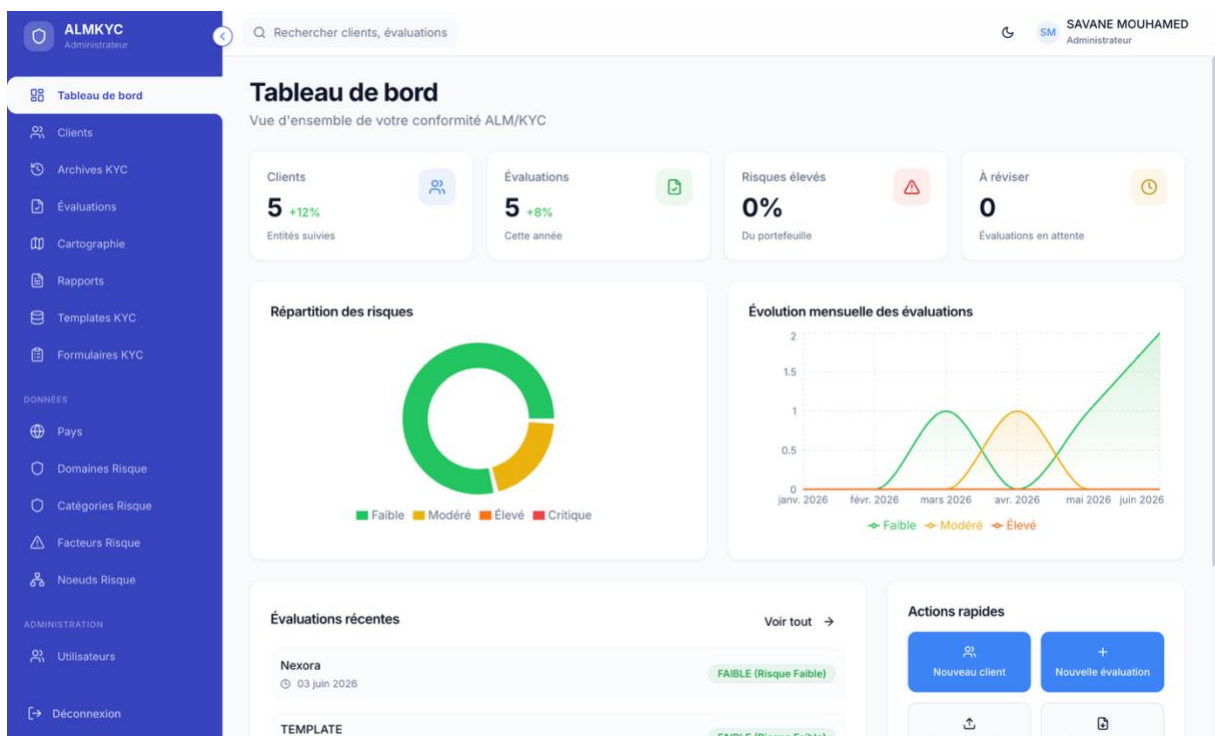


Figure 22 - Page tableau de bord

ALMKYC Administrateur

Rechercher clients, évaluations

SAVANE MOUHAMED Administrateur

Clients

Gérez vos entités clientes et leurs informations

+ Nouveau client

Rechercher par nom...

Tous les types Tous

- Nexora Sénégal SARL** Brouillon — Étape 2/3
Dernière mise à jour : 03 juin 2026, 13:06
- Société anonyme** Brouillon — Étape 2/3
Dernière mise à jour : 02 juin 2026, 14:03
- medico** Brouillon — Étape 3/3
Dernière mise à jour : 23 avr. 2026, 14:53
- RAS** Personne Morale Risque Faible 1/4 V: 1.00
Actif
- TEMPLATE** Personne Morale Risque Faible 1/4 V: 1.00
Actif
- Nexora** Personne Morale Risque Faible 1/4 V: 1.00
Actif
- NEXORA** Personne Morale Risque Faible 1/4 V: 1.00
nexora@ci.com • Actif

Tableau de bord

Clients

- Archives KYC
- Évaluations
- Cartographie
- Rapports
- Templates KYC
- Formulaires KYC

DONNÉES

- Pays
- Domaines Risque
- Catégories Risque
- Facteurs Risque
- Noeuds Risque

ADMINISTRATION

- Utilisateurs
- Déconnexion

Figure 23 - Visualisation de la liste des clients

ALMKYC Administrateur

Rechercher clients, évaluations

SAVANE MOUHAMED Administrateur

Nexora PM KYC Dynamique

Pas d'email • Actif

Réévaluer Fiche DOS Modifier

Vue d'ensemble Détails KYC Évaluations 1

Identification & Risque Personne Morale

Données structurées issues du template KYC

Personne morale

RAISON SOCIALE Nexora	SIGLE NXS	FORME JURIDIQUE SARL (Société à Responsabilité Limitée)
ZONE GÉOGRAPHIQUE Corée du Nord	N° COMPTE CONTRIBUTABLE 1234567A2	DATE DE DÉCLARATION FISCALE 1999-07-13
N° REGISTRE DE COMMERCE SN-DKR-2026-B-12345	DATE D'INSCRIPTION 1999-06-03	SECTEUR D'ACTIVITÉ Horticulture et reproduction des plantes

ADRESSE & CONTACT (CANAUX)

B.P. BP 12500 Dakar	SIÈGE SOCIAL 15 Avenue Léopold Sédar Senghor, Dakar, Sénégal	JUSTIFICATIF DU SIÈGE SOCIAL Contrat de bail commercial
------------------------	---	--

Tableau de bord

Clients

- Archives KYC
- Évaluations
- Cartographie
- Rapports
- Templates KYC
- Formulaires KYC

DONNÉES

- Pays
- Domaines Risque
- Catégories Risque
- Facteurs Risque
- Noeuds Risque

ADMINISTRATION

- Utilisateurs
- Déconnexion

Figure 24 - Visualisation des détails d'un client

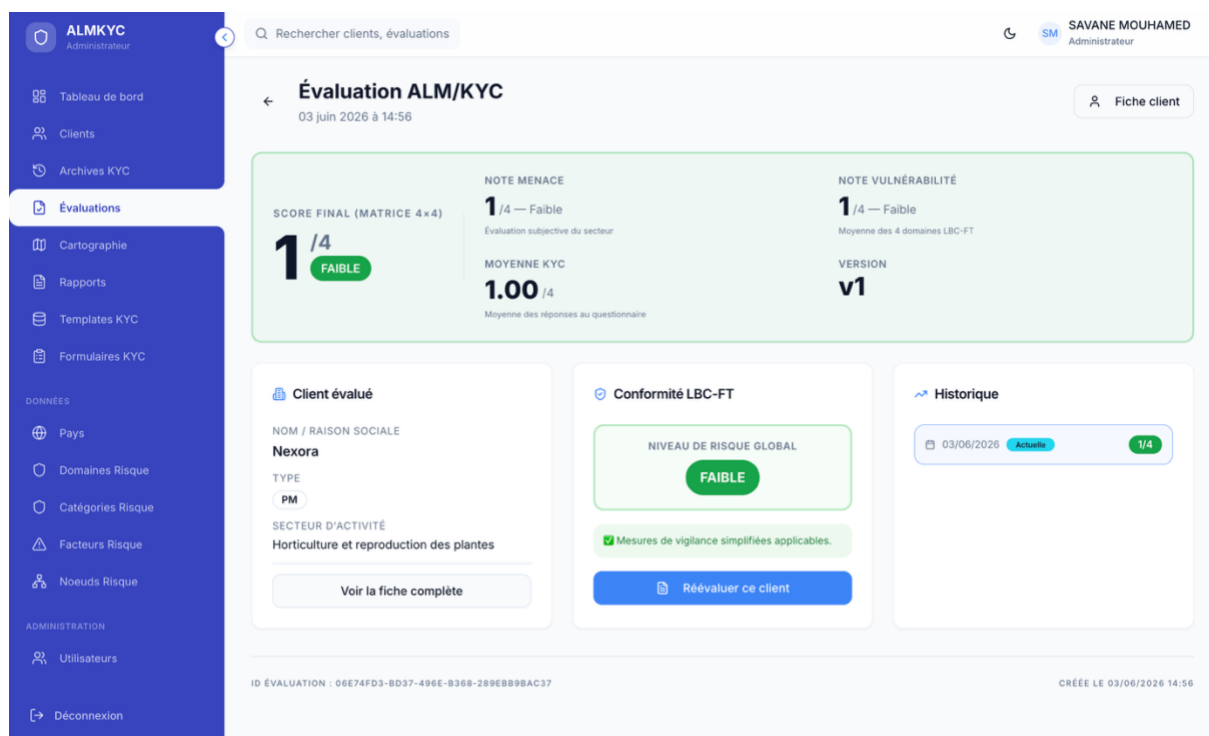


Figure 25 - Visualisation des détails de l'évaluation d'un client

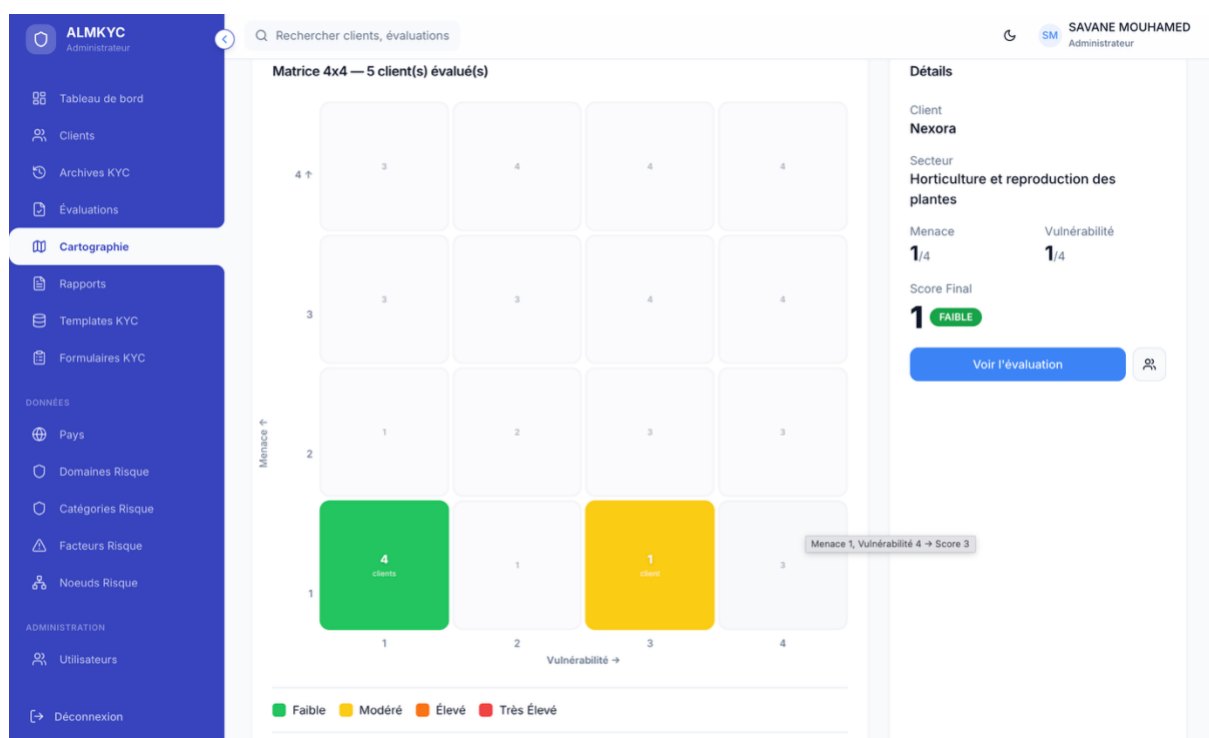


Figure 26 - La matrice de croisement Vulnérabilité x Menace

ALMKYC

Administrateur

Rechercher clients, évaluations

SM

SAVANE MOUHAMED

Administrateur

Cartographie

Rapports

Templates KYC

Formulaires KYC

Données

Pays

Domaines Risque

Catégories Risque

Facteurs Risque

Noeuds Risque

Administration

Utilisateurs

Mon Abonnement

Journal d'audit

Référentiels

Paramètres

Déconnexion

Mes abonnements

ACTIF

STANDARD

STANDARD

25 000 FCFA/mois

Période d'abonnement

10/02/2026

545 jours restants

12/12/2027

CAPACITÉ

Jusqu'à 5 utilisateurs

FONCTIONNALITÉS

Toutes les fonctionnalités KYC & ALM

Renouveler

Se désabonner

Supprimer

Licences disponibles

STANDARD

25 000 FCFA / mois

Licence standard

Jusqu'à 5 utilisateurs

Gestion des clients & KYC

Rapports réglementaires (DOS)

Cartographie des risques

Figure 28 - Page d'abonnement pour un cabinet

ALMKYC

Administrateur

Rechercher clients, évaluations

SM

SAVANE MOUHAMED

Administrateur

Tableau de bord

Clients

Archives KYC

Évaluations

Cartographie

Rapports

Templates KYC

Formulaires KYC

Données

Pays

Domaines Risque

Catégories Risque

Facteurs Risque

Noeuds Risque

Administration

Utilisateurs

Déconnexion

Domaines de Risque ALM/KYC

Les 4 piliers réglementaires GIABA pour l'évaluation des risques

Les codes CLIENTS, PRODUITS_SERVICES, CANAUX et ZONES_GEO sont les 4 piliers GIABA imposés par la norme. Leur code ne peut pas être modifié une fois créé.

Piliers d'évaluation (4)

#	Code	Libellé	Description	Statut	Actions
1	CLIENTS	Clients	—	Actif	...
2	PRODUITS_SERVICES	Produits & Services	—	Actif	...
3	CANAUX	Canaux de distribution	—	Actif	...
4	ZONES_GEO	Zones géographiques	—	Actif	...

Figure 29 - Les 4 piliers réglementaires GIABA

57

3. Estimation du coût du projet

Le tableau ci-dessous détaille l'estimation du coût du projet, incluant les dépenses liées aux logiciels, au matériel nécessaire et aux frais de services professionnels associés. Le montant total de ce projet s'élève à **19 877 600,00 F CFA**.

Tableau 16 - Tableau récapitulatif des infrastructures et de leurs prix

Désignation	Quantité	Prix unitaire (FCFA)	Total (FCFA)
	Infrastructures utilisés		
Ordinateur	01	3 539 000,00	3 539 000,00
VPS	01	80 000,00 / mois	320 000,00
Stockage objet (MinIO / S3)	01	29 500,00 / mois	118 000,00
Total Matériel			3 977 000,00
	Services professionnels		
Développeur Full-stack	120(j)	70 000,00 / j	8 400 000,00
Ingénieur DevOps	90(j)	70 000,00 / j	6 300 000,00
Connexion internet	120(j)	10 000,00 / j	1 200 000,00
Total Services Professionnels			15 900 000,00
Total Générale (FCFA)			19 877 000,00

III. DISCUSSION DES RÉSULTATS

Ce chapitre présente les réussites du projet ainsi que les limites et les perspectives de celui-ci.

1. Réussites du projet

Le développement de la plateforme LBCFT a permis de concrétiser l'ensemble des objectifs fonctionnels et techniques définis dans le cahier des charges initial. L'analyse des résultats obtenus, confrontée aux exigences réglementaires de la LBC/FT et aux bonnes pratiques de génie logiciel, révèle des réussites significatives tant sur le plan métier que sur le plan de l'architecture logicielle. La présente section propose une analyse critique et détaillée de ces résultats, en s'appuyant exclusivement sur les éléments réellement implémentés dans le système.

1.1. Conception et réalisation de la plateforme

Ce mémoire a porté sur la conception et le développement d'une plateforme numérique d'évaluation du risque de conformité réglementaire dans le cadre de la lutte contre le

blanchiment de capitaux et le financement du terrorisme. La solution proposée répond à la nécessité de moderniser les processus d'évaluation des risques en automatisant les traitements, en centralisant les données et en améliorant la traçabilité des opérations.

1.2.Déploiement et apports de la solution

La plateforme a été déployée avec succès et est aujourd'hui opérationnelle. Les résultats obtenus démontrent sa capacité à faciliter les évaluations de risques, à améliorer la gestion des dossiers de conformité et à fournir des outils d'aide à la décision adaptés aux besoins des professionnels du secteur. Cette réalisation constitue une contribution concrète à la transformation numérique des dispositifs de conformité réglementaire.

2. Limites et perspectives du projet

Malgré les résultats positifs présentés dans la section précédente, la plateforme LBCFT, comme tout système logiciel issu d'un projet de fin d'études réalisé dans un délai contraint de six mois, présente un certain nombre de limites qui méritent d'être identifiées et analysées avec rigueur. Ces limites, loin de remettre en cause la pertinence du projet, constituent autant de pistes d'amélioration pour les futures évolutions de la plateforme.

2.1.Limites techniques

La première limite technique significative concerne le modèle de *scoring* actuel. Le calcul des scores de vulnérabilité repose sur une moyenne arithmétique simple de tous les facteurs évalués au sein de chaque domaine, sans pondération différenciée. Le champ *weight* est certes prévu dans le schéma des facteurs de risque (*RiskFactor*), mais il n'est pas exploité dans la logique de calcul implémentée dans *calculateRisk*. Cette approche, bien que conforme au document de référence « Support Atelier La Fiduciale », implique que tous les facteurs d'un même domaine ont un poids identique dans le calcul, alors que certains facteurs (comme le statut de Personne Politiquement Exposée) peuvent objectivement présenter une incidence plus forte sur le niveau de risque global.

La deuxième limite réside dans l'architecture monolithique du backend. Bien que l'organisation modulaire de NestJS offre une bonne séparation logique des préoccupations, l'ensemble du système s'exécute comme un processus unique au sein d'un seul conteneur Docker. Cette architecture monolithique, adaptée à la phase actuelle du projet, pourrait devenir un goulot d'étranglement en cas de montée en charge significative, notamment si le nombre de cabinets et d'évaluations simultanées augmente de manière importante.

La quatrième limite concerne la matrice de croisement Vulnérabilité × Menace, qui est codée en dur dans le service *KycEvaluationsService* sous forme d'un tableau JavaScript. Bien que

cette approche garantisse la cohérence et la rapidité du calcul, elle ne permet pas aux administrateurs de modifier la matrice sans intervention directe dans le code source, ce qui limite la flexibilité du système face à d'éventuelles évolutions réglementaires de la méthodologie d'évaluation.

2.2.Limites fonctionnelles

Sur le plan fonctionnel, la plateforme ne propose pas encore de mécanisme de screening automatisé contre les listes de sanctions internationales, les listes de Personnes Politiquement Exposées (PPE) ou les listes de gel des avoirs. Cette fonctionnalité, bien que non incluse dans le périmètre initial du projet, est pourtant centrale dans les dispositifs de conformité LBC/FT des solutions commerciales existantes.

L'absence de version mobile constitue également une limite fonctionnelle identifiée dès l'avant-propos du mémoire. Bien que l'interface web soit responsive grâce à Tailwind CSS, une application mobile native ou hybride offrirait une expérience utilisateur optimisée pour les agents de terrain qui réalisent les vérifications KYC en déplacement.

Le système de notification se limite actuellement à l'envoi d'e-mails (bienvenue, réinitialisation de mot de passe) via le service SMTP. Il ne comporte pas encore de système de notification en temps réel (WebSocket) pour alerter les utilisateurs des événements critiques : nouvelles évaluations à risque élevé, expiration prochaine d'un abonnement, documents en attente de vérification ou modifications du barème de risque.

2.3.Perspectives d'évolution

Les perspectives d'évolution du projet sont nombreuses et s'inscrivent dans une logique de montée en maturité progressive de la plateforme. Elles sont organisées ci-après par ordre de priorité et de faisabilité technique.

Amélioration du modèle de **scoring** par des méthodes statistiques et probabilistes. Le mémoire consacre une section à l'étude des méthodes statistiques et probabilistes susceptibles d'améliorer le moteur d'évaluation des risques. La première amélioration envisageable est la normalisation des scores via la formule min-max, qui permettrait de ramener l'ensemble des scores sur une échelle homogène avant agrégation, éliminant ainsi les biais liés à des systèmes de notation hétérogènes lorsque plusieurs sources de données sont combinées. La deuxième amélioration concerne l'utilisation de l'entropie de Shannon pour détecter automatiquement les comportements atypiques des clients. Une faible entropie dans la distribution des réponses d'un client traduirait un comportement stable et prévisible, tandis qu'une entropie élevée pourrait signaler des variations inhabituelles méritant une investigation approfondie. La troisième

amélioration porte sur l'intégration d'un modèle probabiliste bayésien permettant d'estimer dynamiquement la probabilité qu'un client présente un risque élevé en tenant compte de l'historique des évaluations et des nouvelles informations disponibles, offrant ainsi un scoring adaptatif et auto-améliorant.

Intelligence artificielle et apprentissage automatique. L'intégration de techniques d'intelligence artificielle constitue une perspective majeure pour la plateforme. Un modèle de détection d'anomalies, entraîné sur les données historiques des évaluations KYC stockées dans la collection *kyc_evaluations*, pourrait identifier automatiquement les profils clients présentant des patterns inhabituels. Des algorithmes de classification supervisée (forêts aléatoires, gradient boosting) pourraient être entraînés pour prédire le niveau de risque d'un nouveau client à partir de ses caractéristiques, avant même la réalisation complète de l'évaluation KYC, permettant ainsi un pré-screening intelligent. L'exploitation du champ *weight* déjà prévu dans le schéma *RiskFactor* ouvrirait la voie à un *scoring* pondéré auto-calibré, où les poids des facteurs seraient ajustés automatiquement en fonction des données historiques via des techniques d'apprentissage.

Amélioration du workflow de conformité. Le workflow actuel en trois étapes pourrait être étendu par l'ajout d'étapes supplémentaires : revue de second niveau par le responsable de la conformité, approbation hiérarchique pour les clients à risque élevé, mécanisme de réévaluation périodique automatique avec alertes programmées.

Architecture microservices. La migration progressive vers une architecture microservices, facilitée par la modularité existante de NestJS, permettrait de déployer indépendamment les composants critiques (moteur de scoring, gestion documentaire, authentification) avec des stratégies de scaling horizontal différenciées. Cette évolution serait particulièrement pertinente en cas d'extension de la plateforme à d'autres institutions financières de la zone UEMOA.

Amélioration des performances. L'implémentation d'un mécanisme de cache (Redis) pour les données de référence (arbres de risque, formulaires KYC) fréquemment consultées mais rarement modifiées réduirait la charge sur la base de données et améliorerait les temps de réponse, notamment lors des évaluations simultanées de plusieurs clients.

Extension à d'autres institutions financières. Le modèle SaaS multi-tenant de la plateforme la prédispose naturellement à une extension au-delà des cabinets comptables et de conseil, vers les banques, les compagnies d'assurance, les systèmes financiers décentralisés (SFD) et les établissements de microfinance, moyennant un paramétrage des formulaires KYC et des arbres de risque adaptés aux spécificités réglementaires de chaque secteur.

CONCLUSION

Le présent mémoire a porté sur la conception, le développement et la mise en production d'une plateforme numérique d'évaluation du risque de conformité réglementaire dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme. Réalisé au sein de l'entreprise NEXORA, ce projet répond à la nécessité de moderniser des processus d'évaluation encore largement fondés sur des traitements manuels, souvent peu adaptés aux exigences actuelles de traçabilité, de centralisation et de fiabilité des données.

Afin de répondre à cette problématique, une démarche méthodique a été adoptée, combinant l'étude du cadre réglementaire, la modélisation du système et le développement d'une solution adaptée aux besoins des acteurs de la conformité. La plateforme développée permet d'automatiser les évaluations de risques, de centraliser les données, d'améliorer le suivi des dossiers de conformité et de faciliter la production de rapports destinés à l'aide à la décision.

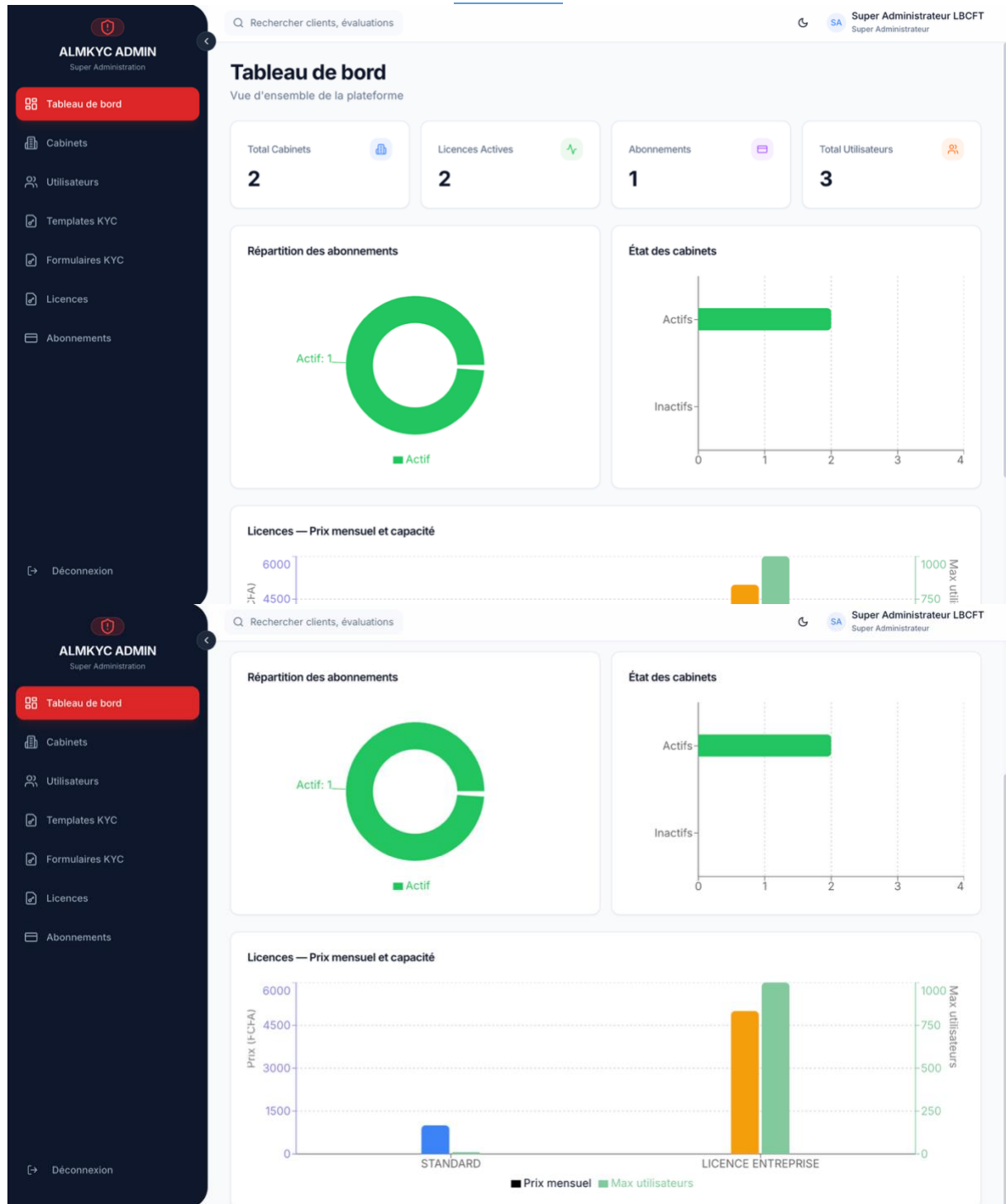
Les résultats obtenus démontrent la pertinence de la solution proposée. La plateforme offre un environnement structuré permettant d'améliorer l'efficacité des évaluations, de réduire les risques d'erreurs liés aux traitements manuels et de renforcer la traçabilité des opérations. Son déploiement en environnement de production confirme sa viabilité et son adéquation avec les besoins opérationnels identifiés.

Au-delà de son apport technique, ce projet contribue à la transformation numérique des pratiques de conformité en proposant une alternative fiable aux méthodes traditionnelles de gestion des risques. Il met également en évidence le rôle des systèmes d'information dans l'amélioration de la gouvernance, de la transparence et de la prise de décision au sein des organisations soumises aux exigences réglementaires.

Les perspectives d'évolution demeurent nombreuses. Elles concernent notamment l'intégration de méthodes avancées d'analyse des risques, l'exploitation de techniques d'intelligence artificielle pour la détection d'anomalies et le scoring prédictif, ainsi que l'extension de la plateforme à d'autres institutions financières et organismes assujettis de l'espace UEMOA.

En définitive, ce travail montre que la digitalisation des processus d'évaluation des risques constitue un levier essentiel pour renforcer l'efficacité des dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme. La plateforme développée représente une contribution concrète à cette démarche en offrant un outil capable d'accompagner durablement les professionnels de la conformité dans leurs missions de contrôle, d'analyse et de prise de décision.

ANNEXE



Annexe 1 - Tableau de bord SuperAdmin

ALMKYC ADMIN

Super Administration

Tableau de bord

Cabinets

Utilisateurs

Templates KYC

Formulaires KYC

Licences

Abonnements

Déconnexion

Rechercher clients, évaluations

SA Super Administrateur LBCFT

Cabinets

Gestion des cabinets

Rechercher par nom ou email...

+ Créer

Rafraîchir

Nom	Email	Téléphone	Actif	Actions
DEKKO GROUP	dekkogroup@lbcft.com	1234567890	Actif	  
ECACI	ecaci.expertise@ymail.com	+225 25 22 01 51 86	Actif	  

Annexe 3 - Page gestion de Cabinet

Rechercher clients, évaluations

SA Super Administrateur LBCFT

Utilisateurs

Gestion de tous les utilisateurs de la plateforme

Rechercher...

Tous les cabinets

+ Créer

Rafraîchir

Nom	Email	Téléphone	Cabinet	Rôle	Statut	Actions
Super Administrateur LBCFT	superadmin@lbcft.com			Super Admin	Actif	   
Mouhamed Savané	savanemouhamed05@gmail.com	0787049961	DEKKO GROUP	Administrateur	Actif	   
COULIBALY Kazana Patrice	ecaci.expertise@ymail.com	+2250101189601	ECACI	Administrateur	Actif	   

Annexe 2 - Page de gestion d'utilisateurs

BIBLIOGRAPHIE

- (FATF), F. A. (2025). *The FATF Recommendations*. Financial Action Task Force.
- Amazon Web Service. (2024, septembre 25). *Let's architect! Building multi-tenant SaaS systems*. Récupéré sur AWS: <https://aws.amazon.com/blogs/architecture/lets-architect-building-multi-tenant-saas-systems/>
- Banque centrale des États de l'Afrique de l'Ouest. (2025, mars 31). *Lutte contre le blanchiment de capitaux et le financement du terrorisme*. Récupéré sur BCEAO: <https://www.bceao.int/fr/reglementations/lutte-contre-le-blanchiment-de-capitaux-et-le-financement-du-terrorisme>
- Banque Mondiale. (2022). *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) — World Bank Framework*. Récupéré sur The World Bank Group: <https://www.worldbank.org/en/topic/financialmarketintegrity/brief/anti-money-laundering-and-combating-the-financing-of-terrorism-aml-cft>
- Banque Mondiale, B. (2015). *National Money Laundering and Terrorist Financing Risk Assessment*. Washington, DC: World Bank Group.
- Centre d'Information Financière de Côte d'Ivoire. (s.d.). *Présentation*. Récupéré sur Centif: <https://www.centif.ci/presentation/>
- ChapsVision. (s.d.). *Solution souveraine LCB-FT : renforcez vos dispositifs*. Récupéré sur ChapsVision: <https://www.chapsvision.com/fr/solution/risques-fraude-conformite-lcbft/>
- ComplyAdvantage. (2024, février 5). *Outil de conformité de LCB-FT pour votre secteur*. Récupéré sur ComplyAdvantage: <https://complyadvantage.com/fr/secteurs/>
- ECA-CI. (s.d.). *Support Atelier La Fiduciale*. Abidjan.
- Expertise France. (2024, juillet 31). *SecFin Africa – Lutter contre les flux financiers illicites en Afrique subsaharienne*. Récupéré sur Expertise France: <https://www.expertisefrance.fr/fr/projets/secfin-africa>
- Fonds Monétaire International (FMI). (2025). *Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)*. Récupéré sur IMF: <https://www.imf.org/en/Topics/Financial-Integrity/amlcft>
- Fonds monétaire international. (2023, avril 26). *Le FMI et la lutte contre le blanchiment des capitaux et le financement du terrorisme*. Récupéré sur FMI: <https://www.imf.org/fr/about/factsheets/sheets/2023/fight-against-money-laundering-and-terrorism-financing>

- Groupe d'Action Financière. (2023). *Les recommandations du GAFI : Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération*. Récupéré sur GAFI/FATF: <https://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/recommandations-gafi.html>
- Groupe Intergouvernemental d'Action contre le Blanchiment d'Argent en Afrique de l'Ouest. (2023). *Rapports d'évaluation mutuelle et analyse des risques régionaux*. GIABA. Récupéré sur GIABA: <https://www.giaba.org/reports/mutual-evaluation/index.html>
- République de Côte d'Ivoire. (2019). *Évaluation nationale des risques de blanchiment de capitaux et de financement du terrorisme*. Abidjan: Comité National de Coordination des Activités de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme.
- République de Côte d'Ivoire. (2023, novembre 23). *Ordonnance n°2023-875 du 23 novembre 2023 relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive*. Récupéré sur Cellule Nationale de Traitement des Informations Financières (CENTIF): https://www.centif.ci/documents/ordonnance_2023_875.pdf
- Signiant. (2025, novembre 17). *The benefits of SaaS multi-tenant architecture*. Récupéré sur Signiant: <https://www.signiant.com/resources/articles/the-benefits-of-saas-multi-tenant-architecture/>

TABLE DES MATIÈRES

RÉSUMÉ.....	III
ABSTRACT.....	III
REMERCIEMENTS	V
AVANTS-PROPOS	VI
SOMMAIRE	VII
LISTE DES SIGLES ET ACRONYMES	VIII
GLOSSAIRE.....	IX
LISTE DES FIGURES	XII
LISTE DES TABLEAUX	XIII
INTRODUCTION.....	1
CHAPITRE I : PRÉSENTATION DE L'ENTREPRISE.....	4
I. PRESENTATION DE LA STRUCTURE D'ACCUEIL (NEXORA)	4
II. ORGANISATION INTERNE DE NEXORA	5
CHAPITRE II : PRÉSENTATION DU PROJET.....	6
I. CADRE GÉNÉRAL DU PROJET	6
II. CONFORMITÉ RÉGLEMENTAIRE, BLANCHIMENT DES CAPITAUX ET FINANCEMENT DU TERRORISME	7
III. CAHIER DE CHARGE ET PLANIFICATION DES TÂCHES	8
CHAPITRE III : ÉTUDE DE L'EXISTANT ET ÉTAT DE L'ART.....	12
I. PRÉSENTATION DE L'EXISANT ET SES LIMITES	12
II. ÉTAT DE L'ART	12
CHAPITRE IV : CONCEPTION DU MODÈLE D'ÉVALUATION DU RISQUE	18
I. IDENTIFICATION ET CLASSIFICATION DES CRITÈRES DE RISQUE	18
II. CONSTRUCTION DU MODÈLE DE SCORING DU RISQUE	21
III. APPROCHE MATHÉMATIQUE D'ÉVALUATION DU RISQUE	24
IV. MÉTHODES STATISTIQUES ET PROBABILISTES POUR L'AMÉLIORATION DU SCORING DE RISQUE 29	
CHAPITRE V : CONCEPTION DE LA PLATEFORME.....	31
I. PRÉSENTATION DES MÉTHODES.....	31
II. ÉTUDE COMPARATIVE ET PRÉSENTATION DES MÉTHODES CHOISIES.....	32
CHAPITRE VI : RÉALISATIONS.....	33
I. DIAGRAMME DE CAS D'UTILISATION.....	33

II. DIAGRAMMES (SÉQUENCE, ACTIVITÉ, CLASSE)	36
CHAPITRE VII : RÉSULTATS.....	44
I. OUTILS ET TECHNOLOGIES UTILISÉS	44
II. PRÉSENTATION DES RÉSULTATS	47
III. DISCUSSION DES RÉSULTATS.....	58
CONCLUSION	63
ANNEXE	XIV
BIBLIOGRAPHIE.....	XX

École Supérieure Africaine des Technologies de l'Information et de la Communication (ESATIC)

Treichville – Zone 3, km 4 BD Marseille – BP 1501 Abidjan 18. Site web :

<https://www.esatic.ci>. courrier : direction.esatic@esatic.ci