AUDEX

Software Requirements Specification

Système d'Audit Intelligent et Automatisé pour sites sensibles

Version 1.0

Auteur principal

Ragnang-Newende Yanis Axe DABO
Développeur Logiciel, Passionné d'IA

Octobre 2025
Ouagadougou, Burkina Faso

Statut : Travail en cours – Phase MVP
Confidentialité : Interne

Table des matières

1 Introduction

Ce document décrit les exigences fonctionnelles et non-fonctionnelles du système **AUDEX** (Audit Expert Automatisé) afin d'assurer un développement cohérent, testé et validé.

1.1 Objectif du document

Fournir une référence unique pour la conception, le développement, les tests et la validation du système AUDEX pour la phase MVP (version 1.0).

1.2 Contexte et justification

Les audits manuels sont longs, hétérogènes et sujets à erreurs. AUDEX vise à réduire la durée d'un audit à vingt minutes sur un jeu d'entrée standard, à améliorer la qualité et la traçabilité des résultats, et à rationaliser la production de rapports.

1.3 Portée du système

AUDEX couvre l'analyse automatisée de données terrain, la détection d'anomalies par IA, le calcul des scores de risque, la génération de rapports PDF, la traçabilité des rapports via blockchain, la consultation via tableau de bord et l'assistant conversationnel. L'analyse de journaux informatiques est prévue pour les étapes ultérieures du projet.

1.4 Définitions et acronymes

— **IA** : Intelligence Artificielle
— **OCR** : Reconnaissance optique de caractères
— **EXIF** : Métadonnées d'images (GPS, date, etc.)
— **RBAC** : Contrôle d'accès basé sur les rôles
— **MVP** : Minimum Viable Product (Produit Minimum Viable)

1.5 Références

— AUDEX – Document de référence
— AUDEX – Proof of Concept (PoC)
— Guide Hackathon Aïobi 2025

2 Vue d'ensemble du système

2.1 Vision générale

AUDEX automatise et fiabilise les audits de sûreté et de cybersécurité. Le système apporte un gain de temps significatif, une amélioration de la qualité d'analyse et une traçabilité renforcée.

2.2 Parties prenantes et rôles

— **Auditeur** : réalise l'audit, annote, génère le rapport
— **Superviseur** : relit, corrige et approuve
— **Administrateur** : gère les utilisateurs, les référentiels et les modèles
— **Lecteur invité** : consulte les rapports signés

2.3 Hypothèses et dépendances

— Connexion Internet disponible de manière intermittente

— Matériel standard utilisable sur le terrain

— Formats de fichiers en entrée : images, PDF, textes, fichiers tabulaires

3 Exigences fonctionnelles

Les fonctionnalités principales sont présentées dans le tableau suivant.

ID	Fonction	Description	Priorité	Version
FR-01	Ingestion	Chargement et traitement de fichiers multimédias (images, PDF, texte, CSV)	Haute	MVP
FR-02	Analyse IA	Détection d'anomalies et classification par catégorie (Incendie, Malveillance, Hygiène, Cyber)	Haute	MVP
FR-03	Scoring	Calcul et agrégation du score de risque par zone et par site	Haute	MVP
FR-04	Rapport PDF	Génération de rapport complet incluant synthèse, visuels et recommandations	Haute	MVP
FR-05	Carte interactive	Visualisation géographique des observations avec filtres pertinents	Moyenne	MVP
FR-06	Assistant	Interaction en langage naturel sur les résultats et recommandations	Moyenne	MVP
FR-07	Blockchain	Enregistrement de l'intégrité du rapport au moyen d'un hachage ancré	Moyenne	MVP
FR-08	Logs IT	Analyse complémentaire de journaux informatiques	Basse	Pilote
FR-09	Authentification	Accès sécurisé et gestion des rôles (RBAC)	Haute	MVP
FR-10	Exports & intégrations	Export CSV/PDF et intégrations externes (API de lecture)	Moyenne	Pilote

Table 1 – Exigences fonctionnelles principales

4 Exigences non-fonctionnelles

ID	Domaine	Exigence	Détail
NFR-P1	Performance	Le traitement d'un lot standard dure au maximum 20 minutes	Jeu d'entrée de référence pour le MVP
NFR-AI1	Précision IA	La précision minimale attendue est de 80%	Objectif cible de 88% au MVP
NFR-S1	Sécurité	Les échanges sont chiffrés en HTTPS et les données stockées avec AES	RBAC pour le contrôle des accès
NFR-R1	Résilience	Le système fonctionne en mode semi-hors-ligne avec cache temporaire	IndexedDB et synchronisation différée
NFR-C1	Compatibilité	L'application est compatible avec Chrome, Edge et Firefox	Versions récentes des navigateurs
NFR-U1	Accessibilité	L'interface est utilisable au clavier et respecte des contrastes lisibles	Bonnes pratiques d'accessibilité

Table 2 – Exigences non-fonctionnelles

5 Architecture du système

5.1 Vue logique

Les principales couches logicielles sont les suivantes :

— **Interface utilisateur** : application web réactive pour la saisie, la cartographie et la consultation des rapports

— **API et services applicatifs** : logique métier pour l'ingestion, l'analyse, le scoring et la génération de rapports

— **Composants IA** : pipelines OCR et vision calculant des détections et des classifications

— **Base de données et stockage** : gestion des entités, des index et des fichiers médias

— **Sécurité et traçabilité** : authentification, contrôle d'accès et ancrage d'intégrité

5.2 Vue de déploiement

L'application web s'exécute sur une architecture client-serveur sécurisée. Le frontend React communique avec une API FastAPI. Les données sont stockées dans une base SQLite pour la phase MVP, puis dans PostgreSQL pour les étapes ultérieures. L'ancrage d'intégrité est réalisé sur un réseau blockchain approprié.

5.3 Composants clés

— Backend applicatif (FastAPI)

— Moteurs et pipelines IA (OpenCV, Scikit-learn)

— Base de données et stockage de fichiers (SQLite → PostgreSQL)

— Interface utilisateur et tableau de bord (React + IndexedDB)

— Module sécurité et traçabilité (JWT, AES, Blockchain)

6 Modèles de données

6.1 Entités principales

Entité	Attribut	Type	Description
Audit	id	Chaîne	Identifiant unique de l'audit
Audit	site_id	Chaîne	Référence du site audité
Audit	statut	Enum	État de l'audit (Brouillon, Revue, Approuvé)
Observation	categorie	Enum	Type d'anomalie (Incendie, Malveillance, Hygiène, Cyber)
Observation	criticite	Entier	Niveau de gravité compris entre 1 et 5
Media	chemin	Chaîne	Chemin du fichier média
Recommandation	priorite	Enum	Priorité de l'action (Haute, Moyenne, Basse)
Utilisateur	role	Enum	Rôle de l'utilisateur (Auditeur, Superviseur, Admin, Lecteur)

Table 3 – Structure des entités principales

6.2 Relations

Un audit contient plusieurs observations. Chaque observation peut comporter plusieurs médias et recommandations. Les utilisateurs disposent de rôles qui déterminent leurs permissions.

7 Architecture logicielle

7.1 Principes de conception

La conception privilégie la séparation claire entre logique métier et accès aux données, la modularité et la testabilité. Les services applicatifs encapsulent la logique de calcul et de règles. Les dépôts de données proposent une interface stable au-dessus du stockage.

7.2 Gestion des erreurs et journalisation

Les erreurs sont gérées par des mécanismes centralisés. Les événements pertinents sont journalisés pour faciliter le diagnostic, la traçabilité et l'observabilité du système en production.

8 Plan de test et critères d'acceptation

8.1 Plan de test

— **Tests unitaires** : parsing OCR/EXIF, règles de scoring, modules de génération de rapport

— **Tests d'intégration** : chaîne de traitement de bout en bout, depuis l'ingestion jusqu'au rapport final

— **Tests de sécurité** : authentification, contrôle d'accès, vérification d'intégrité

— **Tests de performance** : durée totale inférieure ou égale à 20 minutes sur le jeu d'entrée de référence

8.2 Critères d'acceptation

— Le système génère un rapport PDF complet en 20 minutes ou moins pour un lot d'entrée standard

— La cartographie affiche correctement l'ensemble des observations avec un code couleur lisible

— La vérification d'intégrité échoue si le rapport a été modifié après génération

— Le fonctionnement en mode semi-hors-ligne conserve les données durant la session et permet une sauvegarde locale manuelle

9 Roadmap de développement

9.1 Preuve de concept (PoC)

Mise en place du flux principal, de la génération de rapport et d'une première détection IA simple.

9.2 Produit minimal viable (MVP)

Livraison des fonctionnalités principales : analyse IA complète, assistant conversationnel, traçabilité par blockchain et authentification RBAC.

9.3 Phase pilote

Ajout d'un stockage local robuste et d'une synchronisation différée, intégration de l'analyse de journaux informatiques et exposition d'interfaces d'intégration (API).

9.4 Production

Élargissement à des usages mobiles, optimisations IA et intégrations externes, avec supervision et observabilité renforcées.

10 Risques et atténuations

— **Qualité des données terrain** : guider la capture et prévoir une validation manuelle

— **Connectivité limitée** : proposer un mode semi-hors-ligne pour le MVP et une synchronisation différée par la suite

— **Évolution des référentiels** : maintenir des règles configurables et versionnées

— **Performance des modèles IA** : itérations continues sur les jeux de données d'entraînement

11 Annexes

— Modèle de rapport PDF

— Jeux de données de référence

— Règles de conformité initiales

— Diagrammes de flux détaillés