NEOSIS

01

HACKAUDIT - PHASE 2

SYNTHESE

Intégrer une solution multi-agent IA pour assister les commissaires aux comptes dans leurs missions d'audit financier et extra-financier.

ENJEUX CLÉS :

- **Automatisation des tâches répétitives** pour un gain d'efficacité et de précision.
- Renforcement de la **gestion des risques** par des analyses avancées et prédictives.
- Production de **rapports** clairs, **conformes** aux normes (NEP, IFRS) et facilement exploitables.

VALEUR AJOUTÉE :

Optimiser les processus tout en garantissant le **respect des principes déontologiques** et la **transparence** des conclusions.

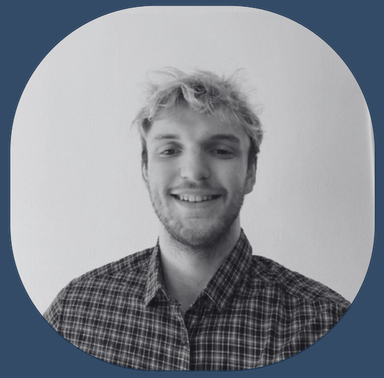
NEOSIS

NEOSIS

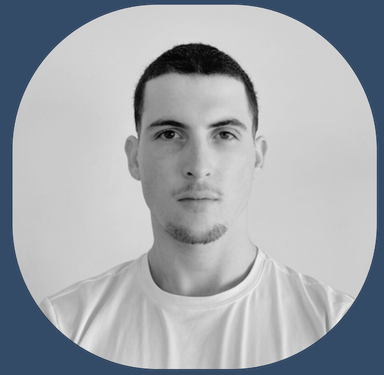
03

NOTRE ÉQUIPE

Titouan Béguère
COORDINATEUR DE PROJET



Léo Maliczak
CHARGÉ DE CONTACTS



Téo Cricelli
RESPONSABLE CAS PRATIQUES

Léa Tching
ANALYSTE DU CONTEXTE

Arthur Perrot
SPÉCIALISTE IA ET INNOVATION

5 étudiants en Master IA et Innovation au sein d'Epitech Digital School

1 - PARAMÉTRAGE ET COLLECTE DES DONNÉES

Action : Paramétrage initial, collecte, nettoyage et structuration des données audit.

Outils : Pandas Profiling, Apache Airflow, Apache Tika et ETL tools

2 - DÉTECTION DES ANOMALIES

Action : Identification des risques et anomalies dans les données.

Outils : XGBoost, Isolation Forest, BERT

3 - RÉCONCILIATION DES COMPTES

Action : Rapprochement et validation des comptes.

Outils : Graph Matching, Machine Learning

4 - DOCUMENTATION ET REPORTING

Action : Synthèse et validation des rapports.

Outils : LLMs, Pandas, Tableau

05

PARAMÉTRAGE ET COLLECTE DES DONNÉES

- **Fiabilité accrue :** **Réduction des erreurs humaines** dans la collecte et le traitement des données.
- **Interopérabilité :** Compatibilité avec **divers systèmes** (ERP, emails, fichiers locaux).
- **Gain de temps :** Automatisation des **tâches répétitives**, permettant aux CAC de se concentrer sur l'analyse à forte valeur ajoutée.

DÉTECTION D'ANOMALIES

- **Réduction des omissions :** **Analyse exhaustive** grâce à des algorithmes avancés (Isolation Forest, XGBoost, BERT).
- **Priorisation intelligente :** Mise en avant des zones à risque pour **optimiser les efforts** du CAC.
- **Transparence et traçabilité :** Alignement avec les **NEP** et **normes sectorielles** pour une documentation claire.

RÉCONCILIATION DES COMPTES

- **Réduction des écarts non résolus :** **Matching** flou et graph matching pour des rapprochements précis.
- **Analyse contextuelle enrichie :** Prise en compte des transactions complexes grâce aux **modèles avancés**.
- **Flexibilité et personnalisation :** Règles **adaptables** selon le secteur ou les spécificités de l'entreprise.

DOCUMENTATION ET REPORTING

- **Conformité systématique :** Validation **automatisée** à chaque étape, **respectant les normes** (NEP, IFRS).
- **Traçabilité complète :** Documents facilement **audités et révisés**.
- **Soutien stratégique :** **Rapports clairs**, prêts à l'emploi pour les parties prenantes.

NEOSIS

RISQUES EXISTANTS

06

RISQUES TECHNIQUES ET FIABILITÉ

- **Faux positifs ou négatifs :** Résultats pouvant nécessiter une **validation humaine** pour éviter des anomalies.
- **Biais algorithmiques : Données d'entraînement** non représentatives pouvant affecter l'analyse.

RISQUES DÉONTOLOGIQUES ET RÉGLEMENTAIRES

- **Automatisation excessive :** L'IA doit rester un outil d'assistance et ne pas remplacer le **jugement professionnel**.

RISQUES DE CONFIDENTIALITÉ SOUS CONTRÔLE

- **Protection des données :** La gestion des données sensibles implique une attention particulière à la **conformité RGPD**.
- **Fuites ou accès non autorisé :** Vulnérabilité accrue aux **cyberattaques**.

RISQUES OPÉRATIONNELS ET D'INTÉGRATION

- **Complexité d'intégration :** Potentielles difficultés pour connecter l'IA avec les **systèmes ERP ou bases existants**.
- **Formation insuffisante :** Les CAC doivent être **formés** pour exploiter efficacement l'outil.

APPROCHES D'ATTÉNUATION DES RISQUES

- **Supervision humaine constante :** Maintenir la validation des résultats par le CAC.
- **Sécurisation des systèmes :** Implémentation de protocoles stricts de chiffrement et de gestion des accès.
- **Formation adaptée :** Programmes de formation pour assurer la maîtrise des outils IA.
- **Audit et documentation rigoureux :** Garantir la traçabilité et la conformité des analyses.

07

Merci

HACKAUDIT 2024

Téo Cricelli - Titouan Béguère - Léo Maliczak - Léa Tching - Arthur Perrot