Transition numérique et innovation – AI Act : enjeux et bonnes pratiques opérationnelles dans les entreprises

INTRODUCTION

- Céline Gentili – Directrice de mission en charge de l'Académie
- Alexis Kasbarian – Responsable du pôle Numérique et Innovation
- Mathilde Briard – Chargée de mission Economie Numérique

- Nathalie Beslay, Avocate, CEO et co-fondatrice de Naaia

Le contexte règlementaire général

Régulation

Mars 2024

2026

Qualification

Quelle catégorie d'opérateur ? + Quelle catégorie de produit d'IA ?

Risques/Sanction

Amendes

Europe: 1,5 % - 7 % CA Mondial exercice précédent

Indemnisation des préjudices

Concurrents
Clients
Class Action

Mouvement des Entreprises de France L'Académie

naaia

AI ACT

LE CALENDRIER

AVRIL 2021	• Proposition de règlement de la Commission Européenne
NOVEMBRE 2022	• Orientation Générale du Conseil de l'Union Européenne
JUIN 2023	• Amendements du Parlement
6 – 8 DÉC. 2023	• Trilogue = Compromis
14 MARS 2024	• Adoption du texte par les eurodéputés

Texte en cours de traduction formelle → 22 AVRIL 2024

Entrée en vigueur : 20 jours après sa publication au Journal officiel de l'UE

Entrée en application:

- 24 MOIS APRÈS L'ENTRÉE EN VIGUEUR
- 6 MOIS POUR LES SIA INTERDITS
- 12 MOIS POUR LES GPAI
- 36 MOIS POUR LES SIA À HAUTS RISQUES (ANNEXE I)

Mouvement des Entreprises de France L'Académie

naaia

QU'EST-CE QU'UN SYSTÈME D'INTELLIGENCE ARTIFICIELLE

Une définition qui a évolué au fil de l'élaboration du texte Européen.

Le 8 novembre 2023, L'OCDE est venu préciser sa définition du SIA laquelle a été reprise dans le texte voté le 13 mars dernier.

Une définition fondée sur <u>les caractéristiques essentielles</u> des systèmes d'IA:

1. **Un système automatisé**
2. **conçu pour fonctionner à différents niveaux d'autonomie,**
3. **qui peut faire preuve d'une capacité d'adaptation après son déploiement**
4. **et qui, pour des objectifs explicites ou implicites**
5. **déduit, à partir des données d'entrée qu'il reçoit**
6. **La manière de générer des résultats tels que:**
   - **Des prédictions**
   - **Du contenu**
   - **Des recommandations**
   - **Des décisions**
7. **qui peuvent influencer les environnements physiques ou virtuels**

<u>Enjeu:</u> retenir des critères suffisamment clairs pour distinguer l'IA des systèmes logiciels plus simples

- Indépendance // humain
- Capacités d'autoapprentissage
- Usage / destination
- Données d'entrée
- L'inférence
- Contexte de fonctionnement

Mouvement des Entreprises de France L'Académie

naaia

LES GRANDS PRINCIPES DE L'AI ACT

Confiance

L'approche de l'UE consiste à donner aux citoyens la confiance nécessaire pour s'approprier ces technologies tout en encourageant les entreprises à les développer.

Contrôle humain

La conception et le développement des systèmes d'IA permettent **un contrôle effectif par des personnes physiques** pendant la période d'utilisation du système IA.

Robustesse technique et sécurité

Les systèmes d'IA sont développés et utilisés de manière à **réduire les dommages involontaires et inattendus**, et à être **résistants** aux tentatives visant une utilisation illégale par des tiers malveillants.

Respect de la vie privée et gouvernance des données

Les systèmes d'IA sont développés et utilisés dans le respect des règles existantes sur la protection de la vie privée et des données personnelles, et répondant à des **normes élevées en termes de qualité et d'intégrité.**

Transparence et explicabilité

Lors de l'utilisation de systèmes d'IA, les utilisateurs doivent être conscients qu'ils interagissent avec une machine afin qu'ils puissent prendre une décision éclairée.

Diversité, non-discrimination et équité

Les systèmes d'IA visent à inclure divers acteurs et à **promouvoir une égalité d'accès** tout en évitant les effets discriminatoires et les préjugés interdits par le droit de l'Union ou le droit national.

Bien-être social et environnemental

Les systèmes d'IA sont durables et **respectueux de l'environnement**, et évitent les incidences à long terme sur **l'individu, la société et la démocratie**.

Mouvement des Entreprises de France L'Académie

naaia

UNE APPROCHE FONDEE SUR LES RISQUES

AI ACT non applicable aux IA
en R&D /prototype
sauf dans le cadre d'essais
En conditions réelles

Risques inacceptables

- Technique subliminale
- Exploitation des vulnérabilités (âge, handicap, situation économique et sociale
- Notation sociale prédictive
- **Système de reconnaissance faciale basée sur des images moissonnées (internet, vidéosurveillance)**
- **Système de reconnaissance des émotions sur le lieu de travail ou d'enseignement sauf pour des raisons médicales ou de sécurité**
- **Système de catégorisation biométrique pour déduire la race, l'appartenance politique ou syndicale, les convictions religieuses ou philosophiques, la vie ou l'orientation sexuelle**
- Système d'identification biométrique en temps réel dans les espaces publics à des fins repressives sauf exceptions (enlèvement, abus sexuel, terrorisme, anticriminalité)

SIA interdits

Risques élevés

- SIA = **produit couvert par les actes législatifs d'harmonisation énumérés à** l'Annexe I s'il doit être soumis à une évaluation de la conformité par un tiers

Ex: Ascenseurs, Equipements de protection, machines, jouets, dispositifs médicaux et dispositifs médicaux de diagnostic in vitro …

- SIA = incidence préjudiciable significative sur la santé, la sécurité et les droits fondamentaux. Les domaines et les cas d'usages concernés sont listés à l'Annexe III de l'AI ACT

Biométrie, infrastructures critiques, éducation, travail, emploi, accès et droit aux services et prestations sociales essentielles (Banque, Assurance, Crédit, Assurance Vie, Assurance ***maladie,*** *solvabilité)…*

SIA à haut risque

Risques spécifiques

- Interactions avec des personnes physiques
- Contenu généré par l'IA tel que texte, audio, vidéos et images
- Reconnaissance des émotions ou de catégorisation biométrique non interdits
- Génération de contenu: Hypertrucage ou information sur des questions d'intérêt public

Risques minimes

Il s'agit de tous les autres systèmes d'IA qui ne présentent pas de risques inacceptables, de risques élevés ou de risques spécifiques

Autres SIA

Risque systémique

- Capacité d'impact élevée (Guidance Commission)
- Puissance de calcul/entrainement
- > 10 Tera 25 FLOPS

Modèles d'IA à usage général

Sans risque systémique

Mouvement des Entreprises de France L'Académie

naaia

LES SYSTEMES D'IA A HAUT RISQUE

SIA relevant de l'Annexe I

✓ Produit couvert par un acte législatif d'harmonisation de l'Union énuméré à l'Annexe 1

les machines, les jouets, les ascenseurs,
les appareils et les systèmes de protection destinés à être utilisés dans des atmosphères potentiellement explosives, les équipements radio,
les équipements sous pression,
les équipements pour bateaux de plaisance, les installations à câbles,
les appareils brûlant des combustibles gazeux,
les dispositifs médicaux et les dispositifs médicaux de diagnostic in vitro.

✓ Produit soumis à une évaluation de la conformité par un tiers (organisme notifié)

Lignes directrices de la Commission (18 mois)
Liste d'exemples pratiques

SIA relevant de l'Annexe III

✓ SIA répertorié dans l'un des domaines suivants:

- Systèmes biométriques
- Gestion et exploitation d'infrastructures critiques
- Emploi, gestion de la main-d'œuvre et accès à l'emploi indépendant
- Éducation et formation professionnelle
- Répression
- Accès et droit aux services privés essentiels et aux services publics et prestations sociales
- Administration de la justice et processus démocratiques
- Migration, asile et gestion des contrôles aux frontières

✓ SIA relevant de l'un des cas d'usages énumérés

Ex: identification biométrique à distance, reconnaissance des émotions, catégorisation biométrique sur la base d'attributs sensibles ou protégés

PAR DÉROGATION

⚠ Sauf pour le profilage des personnes physiques, **ne sont pas classés à haut risque les SIA qui ne présentent pas de risque pour la santé, la sécurité ou les droits fondamentaux des personnes physique**

Notamment:
- Tâche procédurale
- Amélioration du résultat d'une activité humaine
- Prise de constante et mesure sans se substituer à un évaluation humaine préalable
- Tâche préparatoire

Importance de la documentation de l'évaluation du risque

Mouvement des Entreprises de France L'Académie

naaia

LES MODELES D'IA A USAGE GENERAL

Une nouvelle catégorie de produit

Introduite dans la version du Conseil de l'UE en novembre 2022 (système d'IA à usage général)
Reprise par le Parlement dans ses amendements en juin 2023 (Article 28 ter)

Une définition fondée sur les caractéristiques essentielles du modèle:

1. **un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle,**
2. **qui présente une généralité significative et est capable d'exécuter de manière compétente un large éventail de tâches distinctes,**
3. **indépendamment de la manière dont le modèle est mis sur le marché, et qui peut être intégré dans une variété de systèmes ou d'applications en aval,**

Sont expressément exclus les modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur publication sur le marché.

Risque systémique

Un modèle GPAI est considéré comme présentant un risque systémique s'il répond à l'un des critères suivants :

- ❑ Capacités à fort impact (présomption si puissance de calcul > 10^25 FLOPS)
- ❑ Décision de la Commission européenne prise sur la base des critères énoncés à l'annexe XIII

Mouvement des Entreprises de France L'Académie

naaia

LES OPERATEURS DE LA CHAINE DE VALEUR DE L'IA

Fournisseur

Une personne physique ou morale, une autorité publique, une agence ou tout autre organisme

Qui développe ou fait développer un système d'IA ou un modèle d'IA à usage général et **le met sur le marché** ou le **met en service** sous son propre nom ou sa propre marque

A titre onéreux ou gratuit

Distributeur

Toute personne physique ou morale faisant partie de la chaîne d'approvisionnement, autre que le fournisseur ou l'importateur

Qui met un système d'IA à disposition sur le marché de l'Union

Observations

- Une entreprise ou une organisation peut répondre de plusieurs qualifications pour un même système d'IA (ex: fournisseur, distributeur et utilisateur)
- Chaque opérateur doit répondre à un nombre spécifique d'obligations qui dépendront également du système d'IA (hauts risques ou autre)
- Le fournisseur est l'opérateur qui concentre le plus d'obligations
- La qualification de l'opérateur peut évoluer au cours de la vie du système d'IA. Ex: un utilisateur qui procède à des modifications substantielles d'un SIA peut devenir fournisseur

Fournisseur en aval

Un fournisseur d'un SIA **y compris d'un SIA à usage général**

Qui intègre un modèle d'IA

Que ce modèle soit fourni par le même fournisseur ou non

Et verticalement intégré ou fourni par une autre entité **sur la base de relations contractuelles**

Importateur

Toute personne physique ou morale située ou établie dans l'Union

Qui met sur le marché un système d'IA

Qui porte le nom ou la marque d'une personne physique ou morale établie dans un pays tiers

Mandataire

Toute personne physique ou morale située ou établie dans l'Union

Ayant reçu et accepté un mandat écrit d'un fournisseur de système d'IA ou d'un modèle d'IA à usage général

Pour s'acquitter en son nom des obligations et des procédures établies par le présent règlement

Déployeur

Toute personne physique ou morale, autorité publique, agence ou autre organisme **utilisant sous sa propre autorité un système d'IA** sauf lorsque ce système est utilisé dans le cadre d'une activité personnelle à caractère non professionnel

Mise sur le marché :
La première mise à disposition d'un système d'IA sur le marché de l'Union

Mise en service:
La fourniture d'un système d'IA directement au Déployeur en vue d'une première utilisation ou pour usage propre sur le marché de l'Union, conformément à la destination du système

Mise à disposition sur le marché :
Fourniture d'un système d'IA ou d'un modèle d'IA à usage général destiné à être distribué ou utilisé sur le marché dans le cadre d'une activité commerciale

naaia

LA FORMULE DE CALCUL DES OBLIGATIONS

- **Fournisseur**
- **Mandataire**
- **Distributeur**
- **Importateur**
- **Déployeur**

+

- GPAI avec ou sans risque systémique
- SIA à haut risque
- Autres SIA

+

SIA interagissant avec personnes physiques

+

- Génération de contenus textes, audio et images
- Reconnaissance des émotions ou catégorisation biométrique
- Hypertrucage

=

Des exigences à respecter selon le SIA

Des obligations spécifiques à respecter selon les opérateurs

Mouvement des Entreprises de France L'Académie

naaia

LES EXIGENCES APPLICABLES AUX SIA A HAUTS RISQUES

SYSTÈME DE GESTION DES RISQUES

Processus continu et itératif planifié et mis en œuvre tout au long du cycle de vie d'un système d'IA à haut risque, nécessitant une révision et une mise à jour régulières et systématiques.

DONNÉES ET GOUVERNANCE DES DONNÉES

Les systèmes d'IA à haut risque sont développés sur la base d'ensembles de données d'entraînement, de validation et de test, soumis à des pratiques appropriées, notamment des choix de conception pertinents, des processus de collecte de données, un examen visant à identifier les biais potentiels.

DOCUMENTATION TECHNIQUE

Elle est établie de manière à démontrer que le système d'IA à haut risque satisfait aux exigences et à fournir aux autorités nationales compétentes et aux organismes notifiés toutes les informations nécessaires, sous une forme claire et complète, pour évaluer la conformité du système d'IA à ces exigences.

INFORMATION ET TRANSPARENCE

Les SIA à haut risque sont accompagnés de notices d'utilisation dans un format numérique ou autre approprié, contenant des informations concises, complètes, correctes et claires qui sont pertinentes, accessibles et compréhensibles pour les déployeurs.

CONTRÔLE HUMAIN

Nécessité d'une surveillance efficace par les particuliers pendant la période d'utilisation du système d'IA afin de minimiser les risques pour la santé, la sécurité ou les droits fondamentaux.

EXACTITUDE, ROBUSTESSE ET CYBERSÉCURITÉ

Des solutions techniques, telles que des plans de secours et des mesures de sécurité après défaillance, garantissent la robustesse des systèmes d'IA à haut risque.

ENREGISTREMENTS- REGISTRES ET JOURNAUX

Les systèmes d'IA à haut risque doivent permettre techniquement l'enregistrement automatique d'événements ("logs") pendant toute la durée du cycle de vie du système, afin de garantir la traçabilité du fonctionnement du système d'IA.

Mouvement des Entreprises de France L'Académie

naaia

LES OBLIGATIONS PRINCIPALES DES OPERATEURS POUR LES SIA A HAUTS RISQUES

Fournisseur

- Respect des exigences applicables aux SIA à hauts risques
- Système de gestion de la qualité
- Evaluation de la conformité
- Journalisation / registres
- Actions en cas de non-conformité / mesures correctives
- Information des autorités nationales compétentes et le cas échéant de l'organisme notifié
- Coopération avec les autorités compétentes
- Désignation d'un mandataire établi dans l'UE si le fournisseur est établi en dehors de l'UE
- Délivrer de l'information aux fournisseurs en aval

Mandataire

- Exécutions des tâches indiquées dans le mandat
- Vérifier la documentation technique
- Vérifier l'établissement de la déclaration de conformité UE
- Enregistrer le SIA dans la base de données de l'UE

Importateur

- Vérifier la documentation technique
- Vérifier la désignation d'un mandataire par le fournisseur
- Vérifier le marquage CE, la documentation et la notice d'utilisation
- Gérer les signalements d'incidents graves
- Identifier l'importateur sur le SIA

Distributeur

- Coopérer avec les autorités
- Conserver la documentation de conformité
- Vérifier le marquage CE, la documentation et la notice d'utilisation
- Vérifier le respect de leurs obligations par le fournisseur et l'importateur
- Mettre en place des mesures correctives pour les SIA non conformes

Déployeur

- Rendre transparent l'objectif de la collecte des données et Contrôler la pertinence des données d'entrée
- Réaliser une AIPD + une analyse d'impact sur les droits fondamentaux (le cas échéant)
- Tenir des journaux automatiques si ils se trouvent sous leur contrôle
- Informer les personnes physiques de leur interaction avec un SIA
- Mise en œuvre du contrôle humain

Mouvement des Entreprises de France L'Académie

naaia

LES EXIGENCES APPLICABLES AUX SIA A RISQUES SPECIFIQUES

INTERACTION DIRECTE AVEC DES PERSONNES PHYSIQUES

Information d'une interaction avec un système d'IA

GÉNÉRATION DE CONTENUS DE SYNTHÈSE (AUDIO, IMAGE, VIDÉO, TEXTE)

Les résultats produits par le système d'IA doivent être :
- marqués dans un format lisible par machine
- Identifiables comme ayant été générés ou manipulés par une IA

RECONNAISSANCE DES ÉMOTIONS OU CATÉGORISATION BIOMÉTRIQUE

Information des personnes physiques exposées au fonctionnement du système

GENERATION DE CONTENUS À DES FINS D'HYPERTRUCAGE

Le système doit indiquer que les contenus ont été générés ou manipulés par une IA.

Si le contenu fait partie d'une œuvre artistique ou d'un programme créatif: le respect de l'obligation ne doit pas entraver la jouissance de l'œuvre

GENERATION DE CONTENUS À DES FINS D'INFORMATION DU PUBLIC

Le système doit indiquer que les contenus ont été générés ou manipulés par une IA.

Mouvement des Entreprises de France L'Académie

naaia

EXIGENCES APPLICABLES AUX MODELES D'IA À USAGE GÉNÉRAL

Modèle d'IA à usage général

Existe-t-il un risque systémique ?

Présomption: quantité cumulée de calcul utilisée est supérieure à 10^25 FLOPS (opérations en virgule flottante).

Modèles Open source gratuits

NON

OUI

Exclu du champ d'application

R&D, essais (sauf conditions réelles)

Obligations de Transparence

Vis-à-vis des fournisseurs:

- Rédiger et tenir à jour la documentation technique (annexe XI)
- Élaborer et tenir à jour des informations et de la documentation technique pour les fournisseurs aval (Annexe XII)

Vis-à-vis du public:

- Mettre en place une politique visant à respecter la législation de l'Union en matière de droits d'auteur
- Rédiger et mettre à la disposition du public un résumé détaillé du contenu utilisé pour entrainer le modèle

Obligations Supplémentaires

- Effectuer l'évaluation des modèles
- Évaluer et atténuer les éventuels risques systémiques au niveau de l'Union
- Effectuer et documenter des tests contradictoires du modèle
- Documenter et communiquer à la Commission les informations pertinentes sur les incidents graves et les mesures correctives
- Assurer un niveau adéquat de protection de la cybersécurité

Mouvement des Entreprises de France L'Académie

naaia

DES OBLIGATIONS SOUMISES A SANCTIONS

Principe : les Etats membres déterminent le régime des sanctions qui doivent être :
- Effectives
- Proportionnées : prenant en compte la taille et les intérêts des entreprises
- Dissuasives.

Des sanctions prévues par l'AI ACT

EN CAS DE PRATIQUES INTERDITES EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE OU DE NON-CONFORMITÉ AUX DISPOSITIONS RELATIONS AUX DONNEES

€ Amende pouvant aller jusqu'à 35 millions d'euros

jusqu'à 7% du CA annuel mondial total réalisé au cours de l'exercice précédent

EN CAS DE FOURNITURE D'INFORMATIONS INEXACTES, INCOMPLÈTES OU TROMPEUSES AUX ORGANISMES NOTIFIÉS ET AUX AUTORITÉS NATIONALES COMPÉTENTES

€ Amende jusqu'à 7,5 millions d'euros

jusqu'à 1 % du CA annuel mondial total réalisé au cours de l'exercice précédent

EN CAS **D'INFRACTIONS AUX DISPOSITIONS DU REGLEMENT, Y COMPRIS LA VIOLATION DES REGLES RELATIVES AUX GPAI**

€ Amende pouvant aller jusqu'à 15 millions d'euros

jusqu'à 3 % du CA annuel mondial total réalisé au cours de l'exercice précédent

CRITÈRES D'APPRÉCIATION POUR LA FIXATION DE L'AMENDE

- La nature, la gravité et la durée de l'infraction et de ses conséquences
- Amendes par d'autres autorités
- La taille, le chiffre d'affaires annuel et la part de marché de l'opérateur qui commet l'infraction
- Pour chaque catégorie d'infraction, le seuil serait le plus bas des deux montants pour les PME et le plus élevé pour les autres entreprises
- Toute autre circonstance aggravante ou atténuante applicable – exemple : avantages financiers obtenus

Mouvement des Entreprises de France L'Académie

naaia

DEPLOYER UN MODELE OPERATIONNEL DE GOUVERNANCE

1 TRAITER L'URGENCE AVANT FIN 2024

DEPISTER LES SYSTEMES D'INTELLIGENCE ARTIFICIELLE INTERDITS

- Cartographier les SIA Interdits
- Les supprimer ou les mettre en conformité

2 METTRE EN PLACE UN MODELE DE GOUVERNANCE DE L'IA….

- Equipe Cœur de Gouvernance
- Task Force opérationnelle
- Formation des équipes utilisatrices d'IA
- Outil de pilotage centralisé

… POUR SE METTRE EN CONFORMITE

- Cartographier les SIA utilisés dans l'organisation
- Qualifier chaque SIA et son niveau de risque
- Avoir un plan d'actions
- Opérationnaliser la réponse au plan d'actions avec les métiers

3 DEVELOPPER DES CAS D'USAGES COMPLIANT BY DESIGN

- Gouvernance de l'IA par phase de développement
- Former les équipes de Dév
- Tester le niveau de risque du SIA pendant son développement

… POUR TRANSFORMER LA REGLE EN ATOUT COMPETITIF

- La règle au service de la qualité et de la sécurité
- Utiliser la contrainte pour construire la confiance
- Convertir en opportunité relationnelle avec les clients
- Efforts alignés avec le niveau de risques

Mouvement des Entreprises de France L'Académie

naaia

Ce que l’on sait

Un développement exponentiel des usages de systèmes d'intelligence artificielle (SIA)

Des défis majeurs : qualité, sécurité, conformité des produits et des services, IP /assets, responsabilité, réputation, HR

Des enjeux de compétitivité

Des risques identifiés - Opérations, Financiers et Réputation

Un choc règlementaire mondial

Ce qu’il faudrait faire

Gérer les risques sans brider l’organisation ni freiner l’innovation

Piloter la compliance par la valeur

Supporter les métiers et limiter leurs efforts de conformité

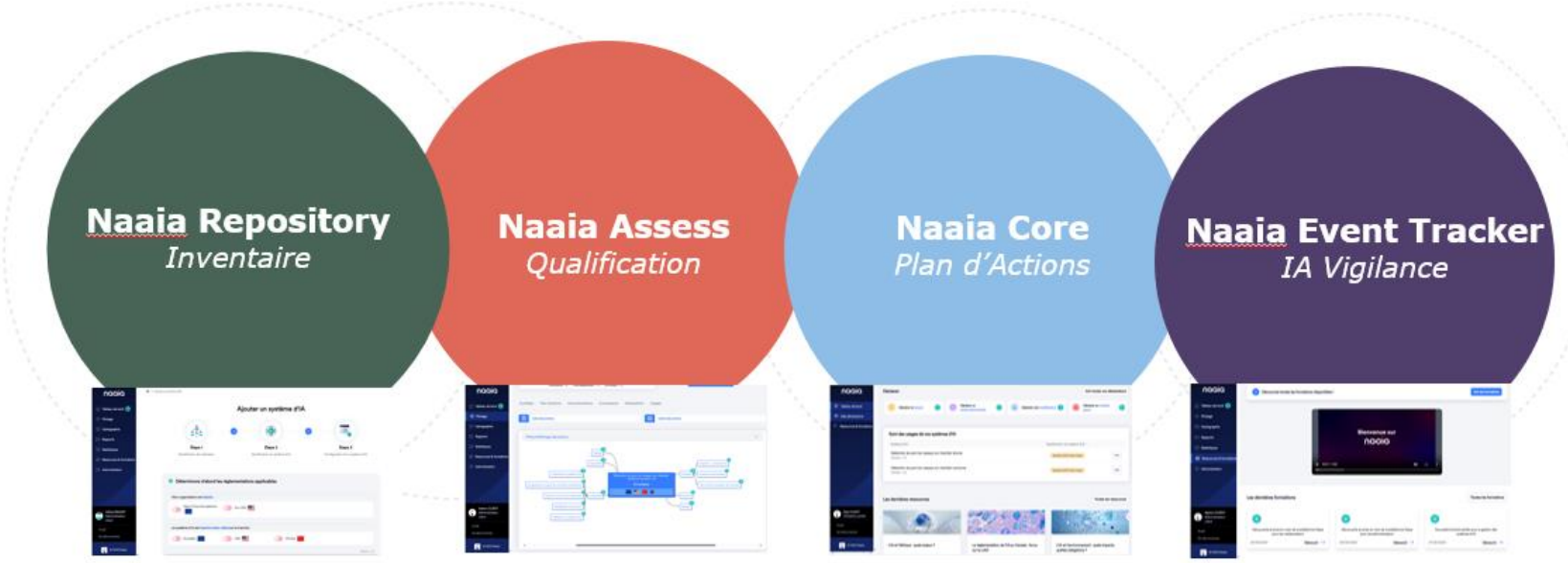
S’intégrer nativement dans les projets

Monitorer les responsabilités

naaia

Les modules fonctionnels

naaia



naaia

QUESTIONS/REPONSES

MERCI DE VOTRE ATTENTION