



# Intelligence artificielle

Vers une approche globale de gestion des risques

28/06/2025

TLP:CLEAR

PAP:CLEAR





# Le projet en synthèse

**La problématique : on ne sait plus par quel bout prendre le problème**

- Une multitude de référentiels et travaux en cours, chacun incomplet, tous incohérents !
- Les institutions ont des domaines de compétences limités
- Les organisations ne segmentent pas : elles doivent tout appliquer !
- Un Règlement IA général en théorie, des projets de normes inapplicables en pratique
  - Lobby rejetant avec force tous les travaux d'harmonisation réalisés depuis des dizaines d'années et ayant fait l'objet de consensus internationaux de tous les domaines au profit d'une approche américaine de sûreté de dispositifs médicaux

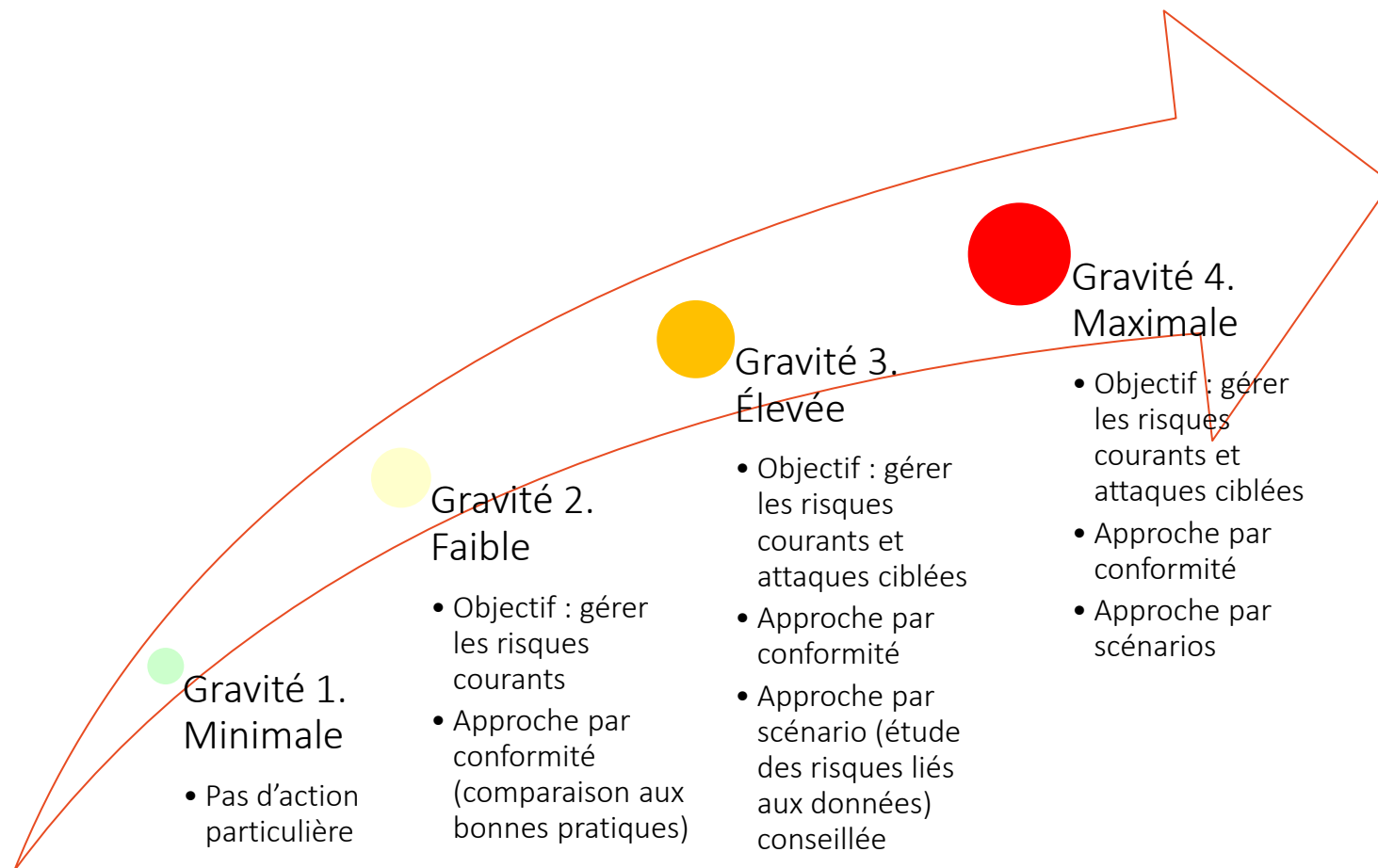
**L'objectif : expliquer par quel bout prendre le problème !**

- Une méthode de gestion des risques de produits ou services qui reposent sur l'IA
- Simple !
- Véritablement **globale** (sécurité de l'information, protection de la vie privée, protection de l'environnement, etc.)
- Basée sur les risques
- Harmonisée et cohérente
- Exploitant les référentiels existants (ne réinventant pas !)
- Flexible et intégrable aux outils et procédures existants



# La logique générale

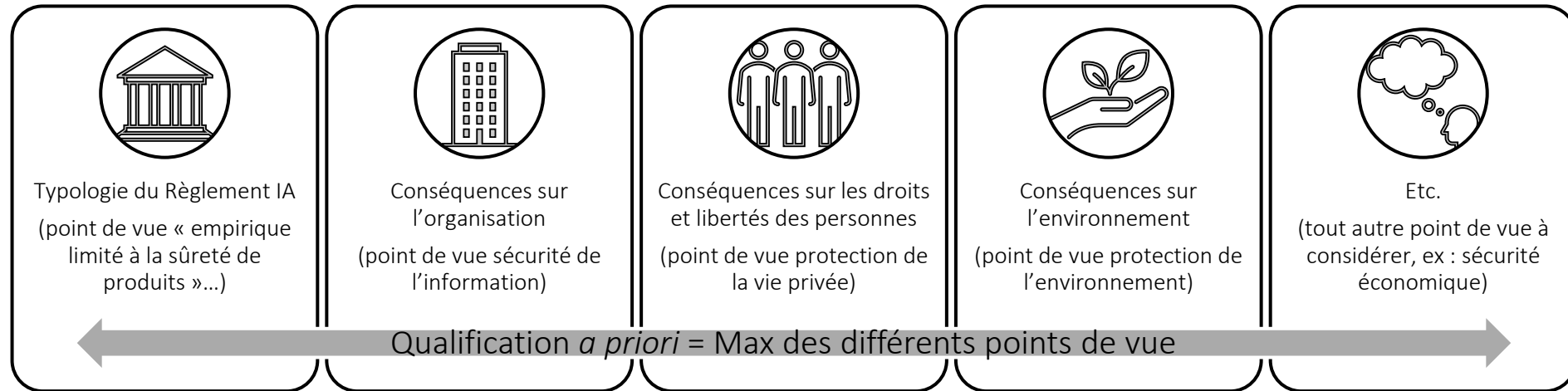
Une approche simple, globale, proportionnée aux risques, et flexible





# Étape 1 : qualification *a priori*

Une échelle pour déterminer la profondeur d'analyse



Gravité	Typologie du Règlement IA	Conséquences sur l'organisation	Conséquences sur les droits et libertés des personnes	Conséquences sur l'environnement	Etc.
1. Minimale					
2. Faible					
3. Élevée					
4. Maximale					



# Étape 2 : approche par conformité

L'objectif : gérer les risques courants

- Problème : aucune harmonisation
  - Les référentiels se ressemblent...
  - Ils emploient tous un classement légèrement différent
  - Les bonnes pratiques sont redondantes et incohérentes
- Solution : un référentiel pivot
  - Des critères de confiance harmonisés
  - Une synthèse des bonnes pratiques
  - Un lien vers les référentiels existants
- Avantages
  - Possibilité de filtrer
  - Utile (voire suffisant) pour homologuer
  - Valorisation des référentiels existants



Gouvernance responsable



Fiabilité et sûreté



Équité



Transparence



Sécurité des informations



Protection des droits et libertés



Maintenance et évolutivité



Interopérabilité



Respect de l'environnement



Accessibilité

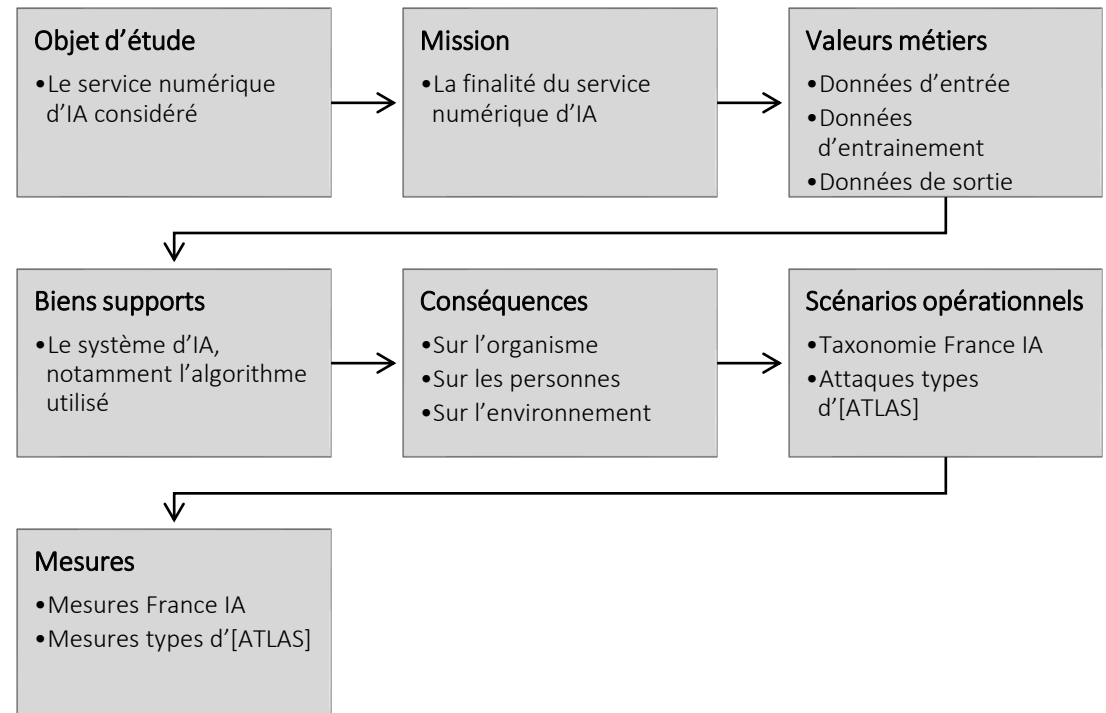


# Étape 3 : approche par scénarios

L'objectif : gérer les attaques ciblées

- Problème : pas d'approche définie
  - Pas de méthode harmonisée pour gérer les risques spécifiques à l'IA
- Solution : spécialiser sa méthode
  - Nos méthodes de gestion des risques de sécurité de l'information fonctionnent
  - Prendre en compte les spécificités de l'IA : données, algorithmes, conséquences au-delà de l'organisme, attaques et mesures spécifiques
- Avantages
  - On n'ajoute pas de nouvel outil
  - On considère réellement les spécificités
  - Directement utile pour homologuer

Exemple : spécialisation d'EBIOS *Risk Manager*





# Pour finir...



# Ressources utilisées

- Images
  - Page de garde : Grid, par Magic Creative, de PIXABAY
  - Logo : Matthieu GRALL expert-conseil
  - Autres : photothèque de MICROSOFT Office