

# Roadmap DE SOUVERAINETÉ NUMÉRIQUE

1

## PARTAGER UNE DÉFINITION

Malgré l'absence d'une définition unique, les référentiels européens et les travaux du Cigref convergent vers ces points :

- Gouvernance & Capital : Anchage stratégique en UE
- Juridique : Immunité aux lois étrangères.
- Données & IA : Contrôle et autonomie des actifs
- Opérationnel : Continuité de service indépendante
- Chaîne d'approvisionnement : Résilience et transparence des composants.
- Technologique : Indépendance (éviter le verrouillage)
- Sécurité & Conformité : Contrôle opérationnel sous juridiction UE
- Durabilité : Autonomie énergétique et environnementale

2

## ANALYSER SES DÉPENDANCES

- Identifier tous vos fournisseurs cloud et logiciels
- Localiser vos données sensibles
- Évaluer les risques de dépendance technologique et économique
- Identifier les contrats fournisseurs contenant des clauses de sortie et de rupture, en privilégiant les évidences et les quick win

3

## ÉVALUER SA POSTURE SÉCURITÉ

- Réaliser une analyse de risques argumentée
- Évaluer le niveau de menace maximal
- Déterminer les besoins de sécurité

4

## GÉRER LA CHAÎNE D'APPROVISIONNEMENT NUMÉRIQUE

- Évaluer la sécurité et la souveraineté des fournisseurs tiers et sous-traitants
- Implémenter des critères de sélection souverains pour les composants logiciels et matériels
- Prévoir des audits réguliers sur la chaîne d'approvisionnement
- Détecter et évaluer les compromissions applicatives par supply chain

5

## MIGRER VERS DE NOUVELLES SOLUTIONS

### ADOPTER DES STANDARDS OUVERTS

- Sélectionner des solutions interopérables
- Éviter le lock-in et garantir la portabilité

### CHOISIR DES SOLUTIONS D'IDENTITÉS SOUVERAINES

- Authentification MFA
- Gestion des comptes privilégiés

### CHOISIR DES SOLUTIONS QUALIFIÉES LE CAS ÉCHÉANT

- SecNumCloud, gouvernance européenne
- Qualification IaaS / SaaS et indices de souveraineté

### PRIVILÉGIER LES COMMUNS NUMÉRIQUES

- Contribuer à l'open source européen
- Développer une expertise interne

6

## GÉRER LE SAVOIR ET LES COMPÉTENCES

- Mettre en place une veille réglementaire, technologique et géopolitique
- Former les achats, décideurs métiers et équipes IT

7

## ACCOMPAGNER LA MIGRATION

- Définir les priorités de migration
- Prévoir des clauses de réversibilité

- Former les équipes techniques

# Annexes



## ERREURS À ÉVITER

- Un SaaS ne devient pas SecNumCloud en utilisant un IaaS SecNumCloud
- Souveraineté ≠ Localisation
- Sous-estimer les solutions européennes
- Migrer sans formation
- Négliger la supply chain et la veille réglementaire
- Oublier qu'une solution open source d'éditeur est avant tout un éditeur
- Le meilleur logiciel n'est pas forcément le plus adapté aux enjeux

## DOCUMENTATION

### 1 ANNUAIRES ET SOLUTIONS

- **Livre blanc sur les PaaS français :** <https://content.rhapsodiesconseil.fr/panorama-des-paas-fran%C3%A7ais>
- **Blueprint des clouds français :** <https://hub.markess.com/blueprint-managed-cloud-services-2024-2025>.
- **Annuaire de solutions françaises :** <https://grenouillemoi.fr>
- **Mise en avant des briques technologiques européennes :** <https://euro-stack.com/>
- **Panorama d'outils et solutions européens :** <https://european-alternatives.eu/>
- **Focus sur les logiciels SaaS européens :** <https://euro-saas.com/>
- **Annuaire des solutions numériques du continent :** <https://www.digital-eu.eu/>
- **Découvrir l'écosystème du logiciel libre et open source français :** <https://annuaire.cnll.fr/>

### 2 LISTE DE CRITÈRES DE SOUVERAINETÉ

- **Framework for buy european regulation - Eurostack**
- **Cloud Sovereignty Framework - European Commission**
- **Et doit sortir en 2026 l'Indice de Résilience Numérique du Clusif**

## RESSOURCES ET CONTACTS

### 1 RÉFÉRENCES OFFICIELLES

- **ANSSI** : Recommandations cloud souverain et référentiel SecNumCloud
- **CLUSIF** : Guide souveraineté et confiance numérique
- **DINUM** : Doctrine "cloud au centre" de l'État

### 2 VEILLE RÉGLEMENTAIRE

- **NIS2** : Directive européenne cybersécurité (applicable octobre 2024)
- **LPM** : Loi de Programmation Militaire française
- **DORA** : Digital Operational Resilience Act (secteur financier)
- **DMA** : Digital Markets Act - Vise à réguler les grandes plateformes

## COMPRENDRE LES ENJEUX

- Enjeux de dépendance contractuelle et réglementaire extra-territoriale
- Enjeux de sécurité
- Enjeux de continuité de service
- Enjeux de coûts et économiques - nos éditeurs sont nos impôts

## CONCLUSION

Dans un environnement numérique complexe, maîtriser ses données et ses dépendances est devenu un **impératif stratégique**. La souveraineté numérique est un **processus continu visant à renforcer l'autonomie et à réduire les risques**. 87 % des entreprises **anticipent sa montée en puissance** : la question n'est plus de savoir s'il faut agir mais comment le faire efficacement.