AYI NEDJIMI Consultants

# SecNumCloud 2026 et EUCS : Guide Complet Qualification

Catégorie : Conformité  Lecture : 4 min  Publié le : 19/01/2026  Auteur : Ayi NEDJIMI

*Guide exhaustif SecNumCloud 2026 et schéma EUCS : exigences techniques référentiel 3.2, processus qualification ANSSI, acteurs qualifiés.*

La doctrine "Cloud au Centre", formalisée par la circulaire du Premier ministre de 2021 et renforcée en 2023, pose le cadre de l'utilisation du cloud par les administrations françaises. Cette politique constitue un levier majeur pour le développement de l'écosystème SecNumCloud.

## Principes directeurs

La doctrine établit plusieurs principes structurants :

**Cloud par défaut** : Le cloud devient le mode d'hébergement de référence pour les nouveaux projets informatiques de l'État. L'hébergement on-premise doit être justifié par des contraintes spécifiques.

**Hiérarchisation des données** : Les données sont classifiées selon leur sensibilité, déterminant le niveau de protection requis et donc le type de cloud autorisé.

**Préférence souveraine** : Pour les données sensibles, les solutions qualifiées SecNumCloud sont privilégiées. L'usage de solutions non-souveraines nécessite une dérogation argumentée.

## Classification des données de l'État

| Niveau | Types de données | Cloud autorisé |
|---|---|---|
| **Niveau 1** | Données publiques, non sensibles | Cloud commercial standard |
| **Niveau 2** | Données non publiques, sensibilité modérée | Cloud certifié ISO 27001 / HDS le cas échéant |
| **Niveau 3** | Données sensibles, stratégiques | SecNumCloud obligatoire |
| **Niveau 4** | Données classifiées | Cloud interministériel spécialisé |

## Mise en œuvre dans les administrations

La doctrine se traduit concrètement par plusieurs mesures :

- **Marchés publics** : Intégration des exigences SecNumCloud dans les appels d'offres
- **Référencement** : Catalogues de services cloud pré-qualifiés pour les administrations
- **Accompagnement** : Programmes de formation et de conseil pour les DSI ministérielles
- **Financement** : Enveloppes dédiées pour les migrations vers le cloud souverain

- **Mutualisation** : Développement d'offres cloud interministérielles

### Impact sur le secteur privé

Bien que la doctrine s'adresse directement aux administrations, elle a un effet d'entraînement sur le secteur privé :

- Les **prestataires de l'État** doivent se conformer aux exigences de leurs donneurs d'ordre
- Les **secteurs régulés** (finance, santé, énergie) s'inspirent de la doctrine pour leurs propres politiques
- Le développement du marché SecNumCloud améliore l'**offre disponible** pour tous
- La **notoriété croissante** du label incite les entreprises privées à s'y référer

## 10 Perspectives 2026-2028

Le paysage du cloud souverain connaîtra des évolutions majeures dans les années à venir. Comprendre ces tendances permet aux organisations d'anticiper et de préparer leur stratégie cloud à moyen terme.

### Évolutions réglementaires attendues

**Adoption de l'EUCS** : Le schéma européen devrait être finalisé et entrer en vigueur, créant un cadre harmonisé au niveau de l'Union. Les modalités d'articulation avec SecNumCloud seront clarifiées.

**Renforcement NIS 2** : L'application complète de NIS 2 accentuera la pression sur les entités essentielles et importantes pour sécuriser leurs systèmes, favorisant l'adoption de solutions qualifiées.

**Évolution DORA** : Le secteur financier devra répondre aux exigences DORA sur les prestataires TIC critiques, créant une demande forte pour des clouds conformes aux standards les plus élevés.

### Tendances technologiques

Plusieurs évolutions technologiques impacteront l'écosystème SecNumCloud :

- **IA souveraine** : Développement d'offres d'IA générative respectant les critères de souveraineté, en réponse au AI Act européen
- **Confidential Computing** : Généralisation des technologies de calcul confidentiel (enclaves sécurisées) renforçant l'isolation des données
- **Post-quantique** : Intégration des algorithmes post-quantiques dans les offres cloud pour anticiper la menace des ordinateurs quantiques
- **Edge computing souverain** : Extension des garanties SecNumCloud aux infrastructures edge pour les cas d'usage latence-sensibles

## Évolution du marché

Le marché français du cloud souverain devrait connaître une croissance soutenue :

- **Consolidation** : Rapprochements entre acteurs pour atteindre la taille critique
- **Enrichissement fonctionnel** : Les offres souveraines rattraperont progressivement les hyperscalers en termes de services managés
- **Spécialisation sectorielle** : Émergence d'offres verticales (santé, finance, secteur public)
- **Internationalisation** : Les acteurs français chercheront à exporter leur savoir-faire en Europe

## Recommandations pour 2026

Pour préparer les évolutions à venir, les organisations devraient :

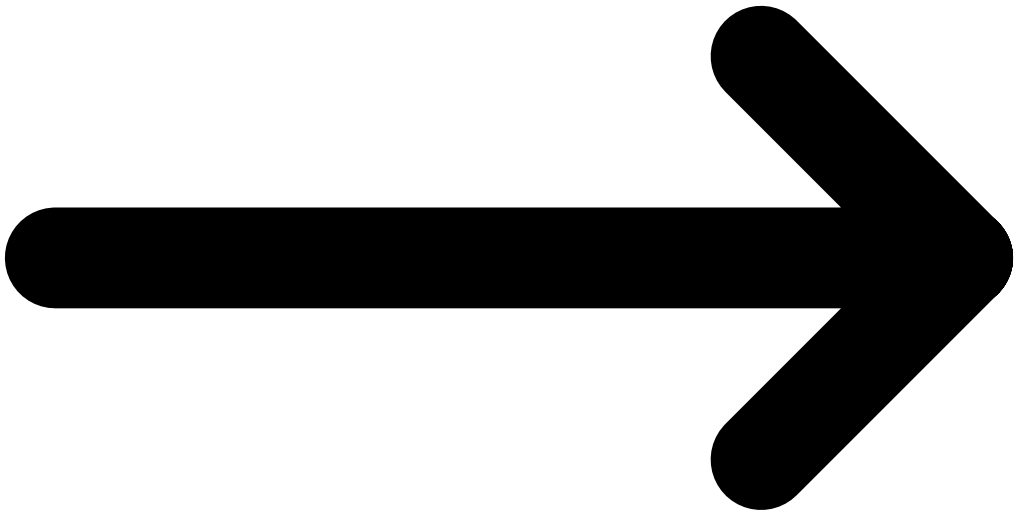
**Actions prioritaires**

- **Cartographier** leurs données sensibles et identifier celles nécessitant un hébergement souverain
- **Évaluer** les offres SecNumCloud disponibles par rapport à leurs besoins
- **Planifier** une feuille de route de migration sur 2-3 ans
- **Former** les équipes aux enjeux de la souveraineté numérique
- **Suivre** les évolutions réglementaires (EUCS, NIS 2, DORA)
- **Budgéter** les investissements nécessaires dans le plan pluriannuel

## Besoin d'accompagnement SecNumCloud ?

Nos consultants spécialisés vous accompagnent dans votre stratégie cloud souverain : évaluation des besoins, sélection des prestataires qualifiés, conduite de la migration et maintien en conformité.

Demander un audit cloud souverain



Pour approfondir ce sujet, consultez notre outil open-source iso27001-toolkit qui facilite l'accompagnement à la certification ISO 27001.

## Questions frequentes

### Comment ce sujet impacte-t-il la securite des organisations ?

Ce sujet a un impact significatif sur la securite des organisations car il touche aux fondamentaux de la protection des systemes d'information. Les entreprises doivent evaluer leur exposition, mettre en place des mesures preventives adaptees et former leurs equipes pour faire face aux risques associes a cette problematique.

### Quelles sont les bonnes pratiques recommandees par les experts ?

### Pourquoi est-il important de se former sur ce sujet en 2026 ?

En 2026, la maitrise de ce sujet est devenue incontournable face a l'evolution constante des menaces et des exigences reglementaires. Les professionnels de la cybersecurite doivent maintenir leurs competences a jour pour proteger efficacement les actifs numeriques de leur organisation et repondre aux obligations de conformite.

**Sources et références :** CNIL · ANSSI

Articles connexes

- AI Act 2026 : Guide Conformité Systèmes IA à Haut Risque
- DORA 2026 : Impact sur le Secteur Financier Francais
- ISO 42001 Lead Implementer : Management de l'IA et
- NIS 2 Phase Opérationnelle 2026 : Guide Complet de Mise

## Conclusion

Points clés à retenir

- 10 Perspectives 2026-2028
- Questions frequentes
- Conclusion

**Ayi NEDJIMI Consultants** — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr