Move2Cloud

WHITE PAPER — ÉDITION 2027

CADRE RÉGLEMENTAIRE EUROPÉEN

Cloud Souverain en Europe

Le guide pratique pour comprendre le nouveau cadre réglementaire européen (CADA, Cloud Sovereignty Framework, NIS2, DORA) et bâtir une stratégie cloud conforme, résiliente et maîtrisée.

11 pages · Grille SEAL, feuille de route et auto-évaluation incluses

48	180 M€	SEAL 0→4
critères de souveraineté évalués	premier contrat-cadre européen	niveaux d'assurance à connaître

PRÉPARÉ PAR
Move2Cloud — Conseil Cloud & Infrastructure, Paris

PUBLICATION
Septembre 2026

SOMMAIRE

Ce que vous allez trouver dans ce document

Un parcours en six temps, de la compréhension du cadre réglementaire à la mise en œuvre d'une feuille de route opérationnelle.

À qui s'adresse ce document ? DSI, RSSI, directions des achats et dirigeants d'organisations publiques ou privées françaises et européennes qui évaluent leur dépendance à des fournisseurs cloud non européens, ou qui répondent à des appels d'offres soumis à des exigences de souveraineté.

SYNTHÈSE

L'essentiel en une page

La souveraineté cloud est passée en 2026 du registre des principes à celui des critères d'attribution de marchés publics et des obligations réglementaires.

Depuis avril 2026, la Commission européenne dispose d'un **Cloud Sovereignty Framework** opérationnel : 48 critères, répartis en 8 objectifs de souveraineté, notés selon une échelle de maturité appelée **SEAL** (Sovereignty Effectiveness Assurance Level, de SEAL-0 à SEAL-4). Ce cadre a déjà servi à attribuer un contrat de 180 millions d'euros sur six ans à quatre fournisseurs — dont trois entièrement européens et un, S3NS, qui reste partiellement adossé à une technologie américaine (Google Cloud), ce qui a suscité un débat sur la portée réelle du cadre.

En parallèle, la proposition de **Cloud and AI Development Act (CADA)**, présentée en juin 2026 dans le cadre de l'AI Continent Action Plan, vise à tripler la capacité de data centers de l'Union en cinq à sept ans et introduit son propre système d'assurance à quatre niveaux pour classer les fournisseurs selon la localisation et le contrôle réel des données.

Ces initiatives ne remplacent pas les obligations déjà en vigueur : **NIS2** impose une gestion des risques, une détection 24/7 et des délais de notification d'incident stricts (24h / 72h / 1 mois) aux entités essentielles et importantes ; **DORA** impose aux entités financières une gestion rigoureuse du risque lié aux prestataires ICT tiers, cloud compris.

48
critères répartis en 8 objectifs de souveraineté (Cloud Sovereignty Framework)

180 M€
premier contrat-cadre européen attribué selon ce référentiel (avril 2026)

×3
capacité de data centers européens visée par la CADA d'ici 5 à 7 ans

Pour une organisation française — collectivité, établissement public, PME ou ETI — la question n'est plus « faut-il s'intéresser à la souveraineté cloud ? » mais « à quel niveau SEAL mon architecture actuelle se situe-t-elle, et quel est l'écart avec les exigences de mes marchés, de mes clients ou de mon secteur ? ». Ce document propose une grille de lecture pragmatique pour y répondre.

SECTION 02

Pourquoi la souveraineté cloud devient un sujet de direction générale

Pendant longtemps, la souveraineté numérique a été traitée comme une préoccupation juridique ou politique, périphérique aux choix d'architecture. Trois évolutions rebattent les cartes en 2026 et en font désormais un sujet de gouvernance et de continuité d'activité.

1. La commande publique européenne s'en empare concrètement

Le Cloud Sovereignty Framework n'est plus une déclaration d'intention : il a servi de grille d'évaluation pour attribuer un contrat réel. Les organismes publics qui répondent à des appels d'offres européens, ou qui achètent à des prestataires évalués selon ce référentiel, doivent désormais savoir situer leurs fournisseurs sur cette échelle.

2. Les obligations réglementaires se cumulent et se recoupent

NIS2, DORA et l'EU AI Act ne visent pas spécifiquement la souveraineté, mais convergent vers les mêmes exigences opérationnelles : cartographie des dépendances vis-à-vis des tiers, contrôle du risque de concentration chez un même fournisseur, capacité à démontrer une résilience testée. Une organisation qui traite ces sujets en silos multiplie l'effort ; une organisation qui les traite ensemble, via une seule feuille de route d'architecture, réduit significativement le coût de mise en conformité.

3. Le risque de dépendance a cessé d'être théorique

Les incidents d'infrastructure régionaux survenus en 2026 chez plusieurs hyperscalers ont rappelé qu'une architecture reposant sur une seule zone ou un seul fournisseur, aussi robuste soit-elle contractuellement, reste exposée à un risque de continuité. La question de la souveraineté rejoint alors celle, plus classique, de la résilience : diversification des fournisseurs, réversibilité contractuelle, portabilité technique.

« La localisation des données ne suffit plus à démontrer la souveraineté : c'est la capacité de décision — qui contrôle, qui peut couper l'accès, sous quelle juridiction — qui est désormais évaluée. »

Pour toute organisation exposée à ces exigences — collectivité, établissement public, PME ou ETI — cela se traduit concrètement par une question simple à se poser dès aujourd'hui : **en cas d'audit, de réponse à appel d'offres ou de contrôle réglementaire, seriez-vous en mesure de documenter le niveau de souveraineté réel de votre architecture cloud ?**

SECTION 03

Le nouveau cadre européen : CADA et Cloud Sovereignty Framework

Le Cloud and AI Development Act (CADA)

Présentée par la Commission européenne en juin 2026 dans le cadre de l'**AI Continent Action Plan**, la CADA poursuit trois objectifs : accélérer le développement technologique européen, étendre significativement les capacités de calcul, et garantir l'autonomie stratégique sur les systèmes numériques critiques. Concrètement, le texte vise à **tripler la capacité de data centers de l'Union en cinq à sept ans**, en simplifiant les procédures de permis et en facilitant l'accès au foncier et à l'énergie.

La CADA introduit également son propre système d'assurance à quatre niveaux, fondé sur la localisation et le degré de contrôle des données : **Niveau 1** — hébergement au sein de l'UE ; **Niveau 2** — indépendance vis-à-vis de pays tiers et chaîne logicielle transparente ; **Niveau 3** — propriété et contrôle européens avec sécurité renforcée ; **Niveau 4** — transparence totale et prévention de toute ingérence de pays tiers. Le texte s'adresse aux entreprises, fournisseurs cloud, investisseurs, organismes de recherche et administrations publiques, avec un soutien renforcé pour les secteurs jugés stratégiques.

Le Cloud Sovereignty Framework : 48 critères, 8 objectifs

Déployé opérationnellement en avril 2026, ce référentiel évalue les fournisseurs cloud à l'aide de 48 critères précis, regroupés en huit objectifs de souveraineté, chacun pondéré différemment dans le score final :

OBJECTIF DE SOUVERAINETÉ	POIDS	CE QUI EST ÉVALUÉ
Chaîne d'approvisionnement	20%	Provenance de la conception, de la fabrication et de la distribution du matériel et du logiciel
Stratégique	15%	Localisation et stabilité de l'autorité, de la propriété et du financement
Opérationnelle	15%	Capacité d'acteurs européens à exploiter et supporter le service de façon autonome
Technologique	15%	Standards ouverts, licences, auditabilité, réversibilité (anti-lock-in)
Juridique & juridictionnelle	10%	Exposition à des lois extraterritoriales (ex. Cloud Act américain)
Données & IA	10%	Contrôle des clés de chiffrement et localisation des traitements
Sécurité & conformité	10%	Pilotage de la sécurité par des équipes UE, alignement GDPR / NIS2 / DORA
Durabilité environnementale	5%	Efficacité énergétique et part d'énergies renouvelables

> **À retenir :** la chaîne d'approvisionnement pèse plus lourd que la seule localisation juridique des données — un signal clair envoyé aux fournisseurs qui hébergent en Europe sans maîtriser le matériel ni le logiciel sous-jacents.

SECTION 04

Les niveaux SEAL expliqués simplement

Point essentiel, souvent mal compris : un fournisseur ne reçoit pas une note SEAL unique, mais **huit notes distinctes**, une par objectif de souveraineté.

NIVEAU	SIGNIFICATION
SEAL-0	Aucune souveraineté — contrôle exclusif d'un acteur non-UE, gouvernance entièrement hors juridiction européenne
SEAL-1	Juridictionnel — le droit européen s'applique en théorie, mais son application reste limitée ; des parties non-UE conservent le contrôle
SEAL-2	Souveraineté des données — le droit européen est opposable, mais des dépendances non-UE significatives subsistent
SEAL-3	Résilience numérique — influence européenne réelle, avec seulement un contrôle non-UE marginal
SEAL-4	Pleine souveraineté numérique — contrôle intégral sous droit européen exclusivement

Comment le score est réellement utilisé en appel d'offres

Le mécanisme repose sur deux étapes successives :

1. **Des seuils planchers éliminatoires.** L'acheteur public fixe un niveau SEAL minimal par objectif. Un fournisseur qui passe sous l'un de ces seuils est automatiquement écarté, quelle que soit sa performance sur les autres critères.
2. **Un score pondéré pour classer les candidats restants.** Seuls les fournisseurs ayant franchi tous les seuils sont ensuite classés selon le score pondéré présenté page précédente.

> **Erreur fréquente à éviter :** un fournisseur qui communique « nous sommes SEAL-3 » sans préciser l'objectif concerné ne dit rien de vérifiable — il n'existe ni certification ni organisme d'accréditation SEAL. Seule une évaluation menée par un acheteur public dans le cadre d'une procédure produit un résultat opposable ; une auto-évaluation ne vaut que comme préparation interne. De même, l'hébergement en Europe ne suffit pas : c'est l'autorité de décision réelle sur l'infrastructure qui est déterminante.

SECTION 05

Ce que le premier contrat de 180 M€ nous apprend déjà

En avril 2026, la Commission européenne a attribué un contrat-cadre de 180 millions d'euros sur six ans, permettant aux institutions, agences et organes de l'UE d'acheter des services cloud auprès de quatre lauréats évalués selon le Cloud Sovereignty Framework :

LAURÉAT	COMPOSITION	NIVEAU SEAL ATTEINT
Consortium franco-luxembourgeois	Post Telecom, OVHcloud, CleverCloud	SEAL-3
STACKIT	Allemagne	SEAL-3
Scaleway	France	SEAL-3
Consortium belgo-franco-luxembourgeois	Proximus, S3NS, Clarence, Mistral	SEAL-2

Le choix de la Commission de répartir le contrat entre quatre lauréats — plutôt que de désigner un fournisseur unique — répond explicitement à un objectif de **diversification et de résilience**, afin d'éviter le verrouillage qui résulterait d'une dépendance à un seul prestataire.

Le cas S3NS : un signal à ne pas ignorer

S3NS, coentreprise entre le groupe français Thales et Google Cloud (États-Unis), a été retenue en dépit d'un niveau SEAL-2 seulement — contre SEAL-3 pour les trois autres lauréats. Ce choix a suscité des critiques sur la capacité réelle du cadre à garantir une indépendance vis-à-vis des obligations légales américaines, notamment le Cloud Act.

Pour toute organisation évaluant ses propres fournisseurs, cet épisode illustre un point clé : **un partenariat local ou une présence commerciale en France ne suffit pas à qualifier une offre de « souveraine »** si la technologie sous-jacente et la chaîne d'approvisionnement restent contrôlées par un acteur non européen. La vigilance doit porter sur la réalité technique et juridique, pas uniquement sur le discours commercial.

> **Enseignement pour votre organisation :** lorsque vous évaluez un fournisseur qui se présente comme « souverain », demandez-lui sur quel(s) objectif(s) précis du référentiel il situe son offre, et à quel niveau SEAL. Une réponse vague est en elle-même une information.

SECTION 06

NIS2 et DORA : impacts concrets sur votre architecture cloud

Ces deux textes ne sont pas des cadres de souveraineté à proprement parler, mais leurs exigences opérationnelles recoupent largement celles du Cloud Sovereignty Framework — d'où l'intérêt de les traiter dans une seule démarche.

NIS2 : ce que votre architecture doit démontrer

DOMAINE	EXIGENCE CONCRÈTE
Gestion des risques	Registre de risques documenté par workload, modélisation des menaces, détection de sécurité active 24/7 sur les workloads critiques (au-delà du simple monitoring de performance)
Réponse aux incidents	Alerte précoce sous 24h, notification formelle sous 72h, rapport final sous un mois — avec canaux de communication CSIRT pré-établis
Continuité d'activité	Sauvegardes testées, sites de reprise séparés, exercices annuels, objectifs RTO/RPO documentés par workload critique
Chaîne d'approvisionnement	Inventaire complet des prestataires ICT, dépendances critiques cartographiées jusqu'au deuxième niveau de sous-traitance
Accès & authentification	MFA généralisé sur les comptes à privilèges, gestion automatisée des arrivées / mobilités / départs
Cryptographie	TLS 1.2+ en transit, chiffrement au repos pour les données sensibles, options de clés contrôlées par le client lorsque c'est pertinent

DORA : le cas particulier des entités financières

Pour les établissements financiers et leurs prestataires, DORA impose une gestion structurée du risque lié aux tiers ICT — cartographie des prestataires critiques, clauses contractuelles de sortie et de réversibilité, tests de résilience opérationnelle réguliers. Un fournisseur cloud mal positionné sur les objectifs « chaîne d'approvisionnement » ou « opérationnel » du Cloud Sovereignty Framework est, par construction, plus difficile à sécuriser au sens DORA.

> **Piège fréquent :** traiter NIS2, DORA et la souveraineté cloud comme trois chantiers de conformité distincts, portés par des équipes différentes. Dans la pratique, les plans de reprise d'activité non testés, le manque de formation des instances dirigeantes et la fatigue liée aux alertes de sécurité mal calibrées reviennent comme les trois défaillances les plus fréquemment constatées — et elles se corrigent par une seule feuille de route d'architecture, pas par trois audits séparés.

SECTION 07

Grille d'auto-évaluation : quel est votre niveau d'exposition ?

Avant d'investir dans une migration ou une renégociation contractuelle, commencez par situer votre architecture actuelle sur ces six questions.

1. Savez-vous, pour chaque fournisseur cloud critique, sous quelle juridiction il est réellement gouverné ?

Non pas où les données sont hébergées, mais qui peut légalement en exiger l'accès, et selon quel droit.

2. Votre chaîne d'approvisionnement matérielle et logicielle est-elle documentée ?

Composants, hyperviseur, briques logicielles tierces : savez-vous d'où elles viennent et qui les contrôle ?

3. Pourriez-vous changer de fournisseur cloud principal en moins de six mois ?

La réversibilité contractuelle et technique (formats ouverts, absence de verrouillage propriétaire) est un critère à part entière, pas une option de confort.

4. Vos délais de notification d'incident sont-ils réellement tenables ?

24h pour l'alerte précoce, 72h pour la notification formelle : ces délais supposent une détection déjà en place, pas à construire au moment de l'incident.

5. Avez-vous testé, au cours des douze derniers mois, un scénario de perte régionale ou de défaillance d'un fournisseur ?

Un plan de reprise non testé n'est, au sens réglementaire comme opérationnel, pas un plan de reprise.

6. Si un client ou un financeur vous demandait votre niveau SEAL sur les huit objectifs, sauriez-vous répondre ?

Même une réponse approximative aujourd'hui vaut mieux qu'une absence de réponse le jour d'un appel d'offres.

> **Comment lire vos réponses :** trois « non » ou plus sur ces six questions indiquent généralement un écart significatif entre votre architecture actuelle et le niveau d'exigence désormais attendu sur les marchés publics et réglementés. C'est le point de départ naturel d'un audit de souveraineté cloud.

SECTION 08

Feuille de route en 5 étapes

Une démarche progressive, pensée pour être menée sans interrompre l'activité ni engager de refonte brutale.

1 **Cartographier**

Inventorier les fournisseurs cloud, leur juridiction réelle, les workloads critiques et les dépendances jusqu'au deuxième niveau de sous-traitance.

2 **Positionner**

Évaluer chaque fournisseur critique sur les huit objectifs de souveraineté et estimer un niveau SEAL indicatif par objectif.

3 **Prioriser**

Identifier les écarts qui bloquent réellement un marché, un client ou une obligation réglementaire — plutôt que de viser une souveraineté maximale partout, souvent hors de portée budgétaire.

4 **Sécuriser et tester**

Mettre en place la détection 24/7, les délais de notification NIS2, et tester concrètement un scénario de bascule ou de perte de fournisseur.

5 **Documenter et faire vivre**

Formaliser le niveau de souveraineté atteint dans un dossier réutilisable pour les appels d'offres, les audits et les revues de direction — et le mettre à jour à chaque évolution du cadre réglementaire.

CONCLUSION

Une contrainte réglementaire, ou un avantage compétitif ?

Les organisations qui traiteront la souveraineté cloud comme un projet d'architecture structurant — plutôt que comme une case à cocher administrative — en tireront un avantage réel : plus de résilience opérationnelle, un accès facilité aux marchés publics soumis au Cloud Sovereignty Framework, et une conformité NIS2/DORA obtenue en un seul effort plutôt que trois.

Le cadre européen continuera d'évoluer dans les prochains mois — la CADA est encore au stade de proposition. Mais les fondamentaux (cartographie des dépendances, réversibilité, résilience testée) resteront pertinents quelle que soit la version finale du texte : c'est par là qu'il est raisonnable de commencer dès maintenant.

Move2Cloud	est un cabinet de conseil spécialisé en infrastructure, cloud et transformation IT. Nous accompagnons les organisations dans l'audit, la conception et la sécurisation de leur architecture cloud, avec une attention particulière portée à la conformité et — désormais — à la souveraineté.
Contact	Move2Cloud — Paris · move2cloud.fr
Prochaine étape	Un audit de souveraineté cloud initial permet de répondre en quelques semaines aux six questions de la page 9, avec une feuille de route priorisée et chiffrée.

Sources

Commission européenne, « Proposal for the Cloud and AI Development Act (CADA) », digital-strategy.ec.europa.eu — Commission européenne, « Sovereign Cloud Framework explained », commission.europa.eu, 1er juin 2026 — nlighten, « The EU Cloud Sovereignty Framework Explained: SEAL Levels, Sovereignty Objectives and the Sovereignty Score » — The Register, « Europe picks 4 sovereign cloud providers, but one has Google », 20 avril 2026 — aenix.io, « NIS2 requirements for cloud infrastructure — a checklist for in-scope entities in 2026 », mai 2026 — SoftwareSeni, « DORA, NIS2, and the EU AI Act Are Making Sovereign Cloud Mandatory for Some Workloads ».