AYI NEDJIMI Consultants

Cloud Compliance NIS 2 SecNumCloud ISO 27017 Guide

Catégorie : Cloud Security Lecture : 8 min Publié le : 09/03/2026 Auteur : Ayi NEDJIMI

Guide de conformité cloud NIS 2, SecNumCloud et ISO 27017 : exigences réglementaires, cartographie des contrôles et plan d'action pour les.

Résumé exécutif

La conformité cloud en 2026 repose sur trois piliers réglementaires : NIS 2, SecNumCloud et ISO 27017. Ce guide cartographie les exigences, identifie les recouvrements et propose un plan d'action unifié pour les organisations françaises et européennes.

Le paysage réglementaire de la sécurité cloud s'est considérablement densifié entre 2024 et 2026. La directive NIS 2, transposée en droit français depuis fin 2024, impose des obligations de sécurité renforcées aux entités essentielles et importantes utilisant des services cloud. Le référentiel SecNumCloud de l'ANSSI, dans sa version 3.2, définit les exigences de qualification pour les prestataires de services cloud traitant des données sensibles françaises. La norme ISO 27017 complète ISO 27001 avec des contrôles spécifiques au cloud. Pour les RSSI et responsables conformité, naviguer entre ces trois cadres réglementaires tout en maintenant une infrastructure cloud opérationnelle et sécurisée représente un défi considérable. Après avoir accompagné plusieurs organisations dans leur mise en conformité multi-référentiels cloud, je propose dans ce guide une approche unifiée qui maximise les synergies entre les trois cadres et minimise l'effort de mise en conformité en évitant les redondances entre les exigences communes à NIS 2, SecNumCloud et ISO 27017.

Quelles sont les exigences NIS 2 pour le cloud ?

La *directive NIS 2* (Network and Information Security) élargit considérablement le périmètre par rapport à NIS 1. Les entités essentielles (énergie, transport, banque, santé, infrastructure numérique) et les entités importantes (services postaux, gestion des déchets, industrie alimentaire, fabrication) doivent implémenter des mesures de gestion des risques cyber proportionnées. Pour les environnements cloud, les exigences clés incluent : la **gestion des risques de la chaîne d'approvisionnement** (évaluer la sécurité de vos providers cloud), la **gestion des incidents** (notification sous 24h pour les incidents significatifs), la **continuité d'activité** (PRA/PCA incluant les scénarios de panne cloud), et la **gouvernance** (la direction est personnellement responsable des mesures de sécurité).

L'ANSSI est l'autorité nationale compétente pour la transposition de NIS 2 en France et publie des guides d'accompagnement. L'audit de vos configurations cloud via audit Terraform compliance est une première étape pour évaluer votre niveau de conformité technique.

Exigence NIS 2	Contrôle cloud	AWS	Azure
Gestion des risques	CSPM / Security scoring	Security Hub	Defender for Cloud
Gestion des incidents	Détection et réponse	GuardDuty + IR	Sentinel + Logic Apps
Continuité d'activité	Multi-AZ, cross-region	AWS Resilience Hub	Azure Site Recovery
Supply chain	Évaluation providers	AWS Artifact	Service Trust Portal
Chiffrement	At-rest et in-transit	KMS + TLS	Key Vault + TLS
Contrôle d'accès	IAM, MFA, PAM	IAM + Identity Center	Entra ID + PIM

Mon avis : NIS 2 est une opportunité déguisée en contrainte réglementaire. Les organisations qui traitent la conformité NIS 2 comme un exercice de paperasse rateront l'occasion d'améliorer réellement leur posture de sécurité. Celles qui utilisent NIS 2 comme levier pour justifier les investissements en sécurité cloud auprès de la direction en sortiront renforcées.

Comment obtenir la qualification SecNumCloud ?

Le référentiel *SecNumCloud* version 3.2 de l'ANSSI définit les exigences pour la qualification des prestataires de services cloud. Il s'adresse aux providers (OVHcloud, Outscale, 3DS Outscale ont obtenu la qualification) mais ses exigences impactent aussi les clients qui doivent héberger des données sensibles sur des clouds qualifiés. Les exigences couvrent : la **localisation des données en Europe**, l'**immunité aux lois extraterritoriales** (CLOUD Act, FISA), le **chiffrement** avec des clés sous contrôle exclusif du client ou du prestataire qualifié, la **séparation des environnements**, et des **audits réguliers** par l'ANSSI.

Pour les clients, l'enjeu est d'identifier quelles données doivent être hébergées sur des clouds qualifiés SecNumCloud et lesquelles peuvent rester sur des hyperscalers non qualifiés. La classification des données par niveau de sensibilité est le prérequis : données stratégiques et de défense sur SecNumCloud, données commerciales et opérationnelles sur les hyperscalers avec les contrôles appropriés. Notre guide sur escalade de privilèges IAM cloud détaille les risques IAM spécifiques aux environnements multi-cloud qui incluent des clouds souverains.

Pourquoi ISO 27017 complète ISO 27001 ?

ISO 27017 est un code de bonnes pratiques pour les contrôles de sécurité de l'information des services cloud. Elle complète ISO 27001/27002 avec des contrôles spécifiques : **séparation des environnements multi-tenant**, **effacement sécurisé des données** à la fin du contrat, **transparence des emplacements de traitement**, **responsabilité partagée** documentée entre le provider et le client, et **portabilité des données**. ISO 27017 ajoute sept nouveaux contrôles cloud et des guidances d'implémentation cloud pour trente contrôles ISO 27002 existants.

La certification ISO 27017 se fait en extension de la certification ISO 27001 existante. L'audit porte sur la mise en œuvre effective des contrôles cloud dans votre SMSI. Les mesures de segmentation réseau décrites dans segmentation réseau VLAN firewall et les pratiques de

gestion des secrets via secrets sprawl et collecte sont des contrôles ISO 27017 évalués lors de l'audit. L'AWS Security fournit des ressources complémentaires sur les certifications de sécurité cloud AWS.

Pour un groupe d'assurance en cours de certification ISO 27017, nous avons cartographié les 37 contrôles cloud applicables et identifié que 22 étaient déjà couverts par leur certification ISO 27001 existante. Les 15 contrôles restants concernaient principalement la transparence de la chaîne de sous-traitance cloud, l'effacement sécurisé des données sur les services managés et la portabilité des données entre providers. L'effort de mise en conformité a été de 4 mois au lieu des 12 initialement estimés grâce à cette approche de delta entre les référentiels.

Comment cartographier les contrôles entre les trois référentiels ?

La cartographie inter-référentiels est essentielle pour éviter la duplication d'efforts. NIS 2 article 21 définit dix catégories de mesures de sécurité qui se recoupent largement avec les domaines ISO 27001/27017 et les exigences SecNumCloud. Par exemple, l'exigence NIS 2 de "gestion des incidents" correspond au domaine A.16 d'ISO 27001, au contrôle CLD.12.1.5 d'ISO 27017 et aux exigences de détection et réponse de SecNumCloud. En travaillant par contrôle transverse plutôt que par référentiel, vous implémentez un seul contrôle qui satisfait trois exigences.

L'outillage est crucial pour maintenir cette cartographie vivante. Les solutions GRC (Governance, Risk, Compliance) comme **Vanta**, **Drata** ou **OneTrust** permettent de mapper les contrôles techniques (configurations cloud, policies) vers les exigences de chaque référentiel et de prouver la conformité en continu via des tests automatisés. L'audit IaC via escalades de privilèges AWS automatise la vérification des contrôles techniques directement dans le pipeline de déploiement.

À retenir : La conformité cloud multi-référentiels s'aborde par les contrôles, pas par les référentiels. Cartographiez les exigences NIS 2, SecNumCloud et ISO 27017 sur une matrice commune, identifiez les recouvrements (qui représentent environ 60% des contrôles), et implémentez des contrôles unifiés qui satisfont plusieurs exigences simultanément. Cette approche réduit l'effort de conformité de 40% et garantit une cohérence entre les référentiels.

Faut-il un DPO dédié pour la conformité cloud ?

NIS 2 n'impose pas explicitement un DPO mais exige que la direction soit formée et responsable des mesures de sécurité. En pratique, un **responsable conformité cloud** dédié est nécessaire dès que l'organisation opère plus de 50 comptes ou subscriptions cloud. Ce rôle combine les compétences de RSSI (sécurité technique), de DPO (protection des données), et de compliance officer (conformité réglementaire). Il coordonne les audits, maintient la cartographie des contrôles, suit les évolutions réglementaires et interface avec l'ANSSI et les auditeurs externes. Sans ce rôle, la conformité cloud reste un exercice ponctuel pré-audit au lieu d'un processus continu.

L'impact de la qualification **EUCS** (European Union Cybersecurity Certification Scheme for Cloud Services) en cours d'élaboration par l'ENISA doit être anticipé. Ce schéma européen créera trois niveaux de certification : Basic, Substantial et High, avec des exigences croissantes de sécurité, de transparence et de souveraineté. Le niveau High, équivalent européen de SecNumCloud, imposera vraisemblablement des exigences de localisation des données en UE et d'immunité aux lois extraterritoriales. Les organisations qui se conforment dès maintenant à NIS 2 et SecNumCloud seront bien positionnées pour la transition vers EUCS, les exigences étant en grande partie alignées par design. Surveillez les publications de l'ENISA et participez aux consultations publiques pour anticiper l'impact sur votre stratégie cloud et adapter progressivement votre architecture et vos processus de conformité.

L'automatisation de la conformité via les outils **Policy as Code** est un accélérateur majeur de la mise en conformité cloud. Des outils comme **Cloud Custodian** permettent de définir des politiques de conformité en YAML qui s'exécutent automatiquement : détecter les ressources non conformes, les taguer, envoyer des notifications, et optionnellement les remédier. Combiné avec Terraform Sentinel ou OPA pour la prévention et les dashboards CSPM pour la visibilité, cette approche Policy as Code crée un système de conformité continu qui ne dépend pas d'audits ponctuels pour maintenir la posture requise par les trois référentiels.

Votre organisation a-t-elle réellement cartographié quelles données sensibles sont hébergées dans le cloud, sur quels services, dans quelles régions, et avec quels niveaux de protection correspondant à chaque cadre réglementaire applicable ?

Comment préparer un audit de conformité cloud ?

La préparation d'un audit de conformité cloud nécessite une approche structurée en quatre dimensions. Premièrement, la **documentation technique** : préparez les schémas d'architecture cloud à jour, la cartographie des flux de données, la matrice de responsabilité partagée par service cloud, et les procédures opérationnelles documentées (incident response, change management, access management). Deuxièmement, les **preuves techniques** : exportez les rapports de conformité Defender for Cloud ou Security Hub, les logs d'audit CloudTrail ou Activity Log sur la période concernée, les résultats de scans de vulnérabilités, et les captures d'écran des configurations critiques (MFA activé, chiffrement configuré, backups automatisés).

Troisièmement, les **preuves organisationnelles** : fournissez les comptes rendus de comités de sécurité, les registres de risques à jour, les plans de formation sécurité avec les attestations de participation, les résultats des exercices de continuité d'activité, et les rapports d'incidents de sécurité traités pendant la période d'audit. Quatrièmement, les **tests de contrôles** : démontrez le fonctionnement effectif des contrôles en exécutant des scénarios devant l'auditeur — rotation d'un secret, détection et réponse à une alerte de sécurité simulée, restauration d'une base de données depuis un backup cross-region, révocation d'un accès utilisateur et vérification de son effectivité.

L'erreur la plus fréquente est de considérer l'audit comme un événement ponctuel plutôt qu'un processus continu. Les organisations matures maintiennent un **dossier de preuves permanent** mis à jour automatiquement par les outils GRC (Vanta, Drata) qui collectent les preuves

techniques en continu via les API des cloud providers. Lors de l'audit, le dossier est déjà complet et à jour, réduisant la phase de préparation de plusieurs semaines à quelques jours de revue et de mise en forme finale.

La conformité cloud n'est pas une destination mais un voyage continu. Les référentiels évoluent, les architectures changent et les menaces se transforment. L'approche la plus durable consiste à intégrer la conformité dans les processus quotidiens via l'automatisation Policy as Code plutôt que de la traiter comme un projet ponctuel pré-audit. Les organisations qui maintiennent une conformité continue via des outils GRC automatisés réduisent leur effort de préparation d'audit de soixante-dix pour cent et détectent les dérives de conformité en temps réel au lieu de les découvrir tardivement lors de l'audit annuel.

Sources et références : CISA · Cloud Security Alliance

Conclusion : plan d'action conformité cloud

Structurez votre mise en conformité en cinq phases sur douze mois. Phase 1 (mois 1-2) : inventaire des assets cloud et classification des données par sensibilité. Phase 2 (mois 3-4) : cartographie des exigences NIS 2, SecNumCloud et ISO 27017 sur une matrice de contrôles unifiée. Phase 3 (mois 5-8) : implémentation des contrôles techniques et organisationnels par priorité de risque. Phase 4 (mois 9-10) : audit interne et remédiation des écarts. Phase 5 (mois 11-12) : audit externe de certification et amélioration continue. Cette approche progressive et structurée maximise les synergies entre référentiels et garantit une conformité durable plutôt que ponctuelle.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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