AYI NEDJIMI Consultants

ANSSI ReCyF : NIS2 en pratique, ce qui change pour vous

Catégorie : Cybersécurité Générale Lecture : 5 min Publié le : 25/03/2026 Auteur : Ayi NEDJIMI

L'ANSSI publie le Référentiel Cyber France (ReCyF) le 17 mars 2026. Ayi NEDJIMI analyse ce que NIS2 va vraiment imposer aux entreprises françaises et.

L'ANSSI a publié le 17 mars 2026 le Référentiel Cyber France, dit ReCyF — le document que les DSI et RSSI attendaient pour comprendre concrètement ce que NIS2 va leur imposer. Après des mois de flou réglementaire, c'est désormais noir sur blanc : voici les mesures techniques et organisationnelles attendues lors des inspections ANSSI. Depuis cinq ans que j'accompagne des organisations dans leurs démarches de sécurité, c'est la première fois qu'un texte français donne autant de prise opérationnelle à une équipe sécurité pour structurer son programme. Mais attention — le ReCyF n'est pas encore contraignant de plein droit, et c'est là que beaucoup vont se tromper dans leur interprétation. Voici ma lecture terrain. L'ANSSI publie le Référentiel Cyber France (ReCyF) le 17 mars 2026. Ayi NEDJIMI analyse ce que NIS2 va vraiment imposer aux entreprises françaises et. Ce guide couvre les aspects essentiels de ANSSI ReCyF NIS2 : méthodologie structurée, outils recommandés et retours d'expérience opérationnels. Les professionnels y trouveront des recommandations directement applicables.

Ce que le ReCyF impose réellement

Le ReCyF est le référentiel de mesures de sécurité aligné sur la directive NIS2, publié par l'ANSSI le 17 mars 2026. Il décline en exigences concrètes les obligations des entités importantes (EI) et entités essentielles (EE) soumises à NIS2. Ce n'est pas un guide de bonnes pratiques de plus — c'est le cadre sur lequel l'ANSSI s'appuiera lors de ses inspections pour évaluer la conformité.

Les mesures couvrent cinq domaines : gouvernance de la sécurité, gestion des risques, sécurité des systèmes, gestion des incidents, et continuité d'activité. Pour chaque domaine, le ReCyF distingue les mesures socles obligatoires des mesures renforcées recommandées. Ce qui m'a frappé dans la lecture du texte : les mesures socles ne sont pas révolutionnaires — elles reprennent en grande partie ce que l'ISO 27001 et les guides ANSSI préconisaient déjà. Ce qui change, c'est le caractère opposable. Une organisation qui n'a pas de politique de gestion des actifs formalisée, pas de processus de gestion des vulnérabilités documenté, ou pas de plan de réponse aux incidents testé, sera en défaut caractérisé lors d'une inspection.

L'erreur que vont faire beaucoup d'organisations

Le ReCyF n'est pas automatiquement contraignant. Les organisations qui l'adoptent formellement peuvent s'en prévaloir lors d'inspections comme preuve de leur démarche de conformité — c'est une différence majeure. Beaucoup de DSI vont interpréter cette nuance comme "on peut ignorer le ReCyF pour l'instant". C'est une erreur stratégique.

Voici pourquoi : NIS2 est transposée en droit français depuis le 17 octobre 2024. Les obligations de sécurité s'appliquent dès maintenant pour les entités identifiées. L'ANSSI n'attend pas que le ReCyF soit formellement obligatoire pour conduire des inspections — elle a déjà commencé à notifier des entités. La question n'est donc pas "dois-je adopter le ReCyF ?" mais "suis-je en mesure de démontrer que mon niveau de sécurité est proportionné au risque ?". Le ReCyF est simplement l'outil de preuve le plus efficace disponible aujourd'hui pour y répondre.

Trois priorités opérationnelles immédiates

1. Savoir si vous êtes EE ou EI. Beaucoup d'organisations ignorent encore leur statut NIS2. L'ANSSI a ouvert le processus de notification — si vous n'avez pas encore reçu de notification et que vous opérez dans un secteur critique (santé, énergie, transport, finance, infrastructure numérique, etc.), ne supposez pas que vous êtes exemptés. Vérifiez activement.

2. Cartographier votre écart par rapport aux mesures socles. Prenez les cinq domaines du ReCyF et faites un gap analysis honnête. Pas besoin d'un cabinet externe pour commencer — une feuille Excel avec les 20 mesures socles prioritaires et une auto-évaluation honnête suffit pour identifier les chantiers critiques. Ce que j'observe en audit : les lacunes les plus fréquentes sont dans la gestion des tiers (supply chain sécurité) et la gestion des identités et accès privilégiés.

3. Tester votre plan de réponse aux incidents. NIS2 impose de notifier l'ANSSI dans les 24h suivant la détection d'un incident significatif. La plupart des organisations n'ont jamais testé ce processus. Un exercice de simulation de crise cyber — même minimal — révèle systématiquement des manques critiques : qui décide ? qui notifie ? quelles preuves sont préservées ? Anticiper les scénarios d'attaque les plus probables comme un ransomware ou une compromission de compte est indispensable.

Ce que NIS2 va vraiment changer pour les RSSI

La vraie nouveauté de NIS2 n'est pas technique — c'est la responsabilité personnelle des dirigeants. L'article 20 de la directive impose que les organes de direction approuvent les mesures de gestion des risques et peuvent être tenus personnellement responsables en cas de non-conformité. Pour les RSSI, c'est une arme à double tranchant : d'un côté, vous avez enfin un levier légal pour faire remonter les investissements sécurité jusqu'au CODIR ; de l'autre, si vous n'avez pas documenté vos recommandations et les arbitrages de la direction, vous risquez d'être celui qui absorbe la responsabilité.

Mon conseil terrain : commencez dès maintenant à documenter formellement vos recommandations sécurité et les décisions de la direction qui ne les suivent pas. Ce n'est pas de la protection juridique — c'est de la gouvernance saine. Et si vous êtes RSSI dans une entité NIS2 sans mandat clair ni budget adapté, le ReCyF vous donne enfin les arguments pour changer ça. Nos ressources sur la stratégie de continuité face aux ransomwares et sur le pentest Active Directory s'inscrivent directement dans les exigences de test et de résilience du ReCyF.

Mon avis d'expert
Le ReCyF est le meilleur outil de structuration d'un programme sécurité que l'ANSSI ait publié. Pas parce qu'il est révolutionnaire, mais parce qu'il donne enfin un cadre opposable, en français, calibré pour la réalité des organisations françaises. Les RSSI qui l'utilisent comme feuille de route dès maintenant — même sans obligation formelle — auront une longueur d'avance considérable lors des inspections. Ceux qui attendent que ce soit contraignant de plein droit risquent de se retrouver en défaut au pire moment : après un incident.

Sources et références : CERT-FR · MITRE ATT&CK

Articles connexes

- Cyber Threat Landscape France 2026 : Bilan ANSSI en 2026
- Darkweb Monitoring : Outils et Techniques 2026 en 2026

> Points clés à retenir
>
> - Ce que le ReCyF impose réellement
> - L'erreur que vont faire beaucoup d'organisations
> - Trois priorités opérationnelles immédiates
> - Ce que NIS2 va vraiment changer pour les RSSI
> - Conclusion

FAQ

Qu'est-ce que ANSSI ReCyF ?

ANSSI ReCyF désigne l'ensemble des concepts, techniques et méthodologies abordés dans cet article. Les fondamentaux sont détaillés dans les premières sections du guide.

Pourquoi ANSSI ReCyF NIS2 est-il important ?

La maîtrise de ANSSI ReCyF NIS2 est devenue essentielle pour les équipes de sécurité. Les enjeux et le contexte opérationnel sont développés tout au long de l'article.

Comment appliquer ces recommandations en entreprise ?

Chaque section de cet article propose des méthodologies et des outils directement utilisables. Les recommandations tiennent compte des contraintes d'environnements de production réels.

Conclusion

NIS2 n'est plus une menace lointaine — elle est active, et l'ANSSI a maintenant les outils et le mandat pour inspecter. Le ReCyF publié le 17 mars 2026 est votre guide de conformité. Commencez par identifier votre statut, faites un gap analysis honnête, et concentrez-vous sur les mesures socles : gouvernance, gestion des risques, incidents et continuité. Ce n'est pas un projet de 18 mois — c'est un programme de sécurité que vous devriez avoir engagé hier. Commencez aujourd'hui.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

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