ReCyF V2.5 ANSSI 2026 : Nouveautés et Impact pour les ETI et Fournisseurs NIS2

Le référentiel ReCyF V2.5, publié par l'ANSSI en mars 2026, marque une étape décisive dans la structuration des exigences cybersécurité imposées aux entités essentielles (EE) et importantes (EI) dans le cadre de la transposition française de la directive NIS2. Cette nouvelle version introduit des évolutions substantielles par rapport à la V2.0 : renforcement des exigences de sécurité de la chaîne d'approvisionnement, harmonisation des procédures de notification d'incidents avec le cadre européen ENISA, généralisation de l'authentification forte et mise en cohérence avec MonEspaceNIS2. Pour les ETI fournisseurs d'entités régulées, comprendre ces évolutions n'est plus optionnel : les entités NIS2 doivent désormais transmettre leurs exigences contractuelles à leurs prestataires directs, et ces derniers sont de facto soumis à un niveau d'exigence sans précédent. Ce guide analyse en détail les nouveautés de ReCyF V2.5 et leur impact concret pour les ETI positionnées dans la supply chain des opérateurs critiques français.

Historique du référentiel ReCyF : de l'origine à la V2.5

Le référentiel ReCyF (Référentiel Cybersécurité Fournisseurs) est né d'un constat simple : les entités régulées ne disposaient d'aucun outil standardisé pour évaluer la maturité cybersécurité de leurs fournisseurs. Avant ReCyF, chaque opérateur d'importance vitale (OIV) ou entité NIS1 développait ses propres questionnaires, générant une fragmentation nuisible pour les fournisseurs qui devaient répondre à des dizaines de formats différents.

L'ANSSI a publié la première version de ReCyF en 2023, dans le sillage des travaux préparatoires à la transposition de NIS2 en droit français (loi NIS2 française publiée fin 2024). La V2.0, déployée en 2024, a consolidé le dispositif avec 112 contrôles organisés en 12 domaines, couvrant la gouvernance, la gestion des risques, la continuité d'activité, la détection et la réponse à incident. La V2.5 de mars 2026 est la première révision majeure post-transposition,

intégrant les retours d'expérience des premières évaluations conduites par les EE et les leçons tirées des incidents majeurs de la chaîne d'approvisionnement en 2024-2025.

Chronologie des versions ReCyF

La version initiale de 2023 posait les fondements conceptuels du référentiel avec 95 contrôles. La V2.0 de 2024 a ajouté 17 contrôles supplémentaires, notamment sur la gestion des accès distants et la sécurité des développements. La V2.5 de mars 2026 n'ajoute pas de contrôles en nombre mais restructure et renforce substantiellement 23 contrôles existants, avec une attention particulière portée à la preuve et à l'opposabilité des mesures déclarées.

Différences clés entre ReCyF V2.0 et V2.5

La transition de la V2.0 à la V2.5 n'est pas anodine. Plusieurs domaines connaissent des évolutions structurantes qui modifient le niveau d'effort requis pour atteindre la conformité.

Supply chain renforcée : la cascade des obligations

C'est l'évolution la plus structurante de la V2.5. Là où la V2.0 demandait à l'entité évaluée de "disposer d'une politique fournisseurs", la V2.5 exige désormais la démonstration que cette politique est effectivement appliquée et que les fournisseurs de rang 2 font l'objet d'une évaluation de niveau minimal. Concrètement, une ETI fournisseur d'une EE devra, sous la V2.5, justifier de ses propres processus d'évaluation cyber de ses sous-traitants critiques. Le principe de cascades d'obligations, cœur de l'article 21-4 de NIS2, se matérialise donc dans ReCyF jusqu'au rang 2.

Cette exigence a un impact majeur sur les ETI dont le modèle repose sur une sous-traitance significative : elles doivent mettre en place un programme de qualification cyber de leurs propres fournisseurs, avec des niveaux d'exigences proportionnés à la criticité des services fournis.

Notification d'incidents : harmonisation avec le cadre ENISA

La V2.0 imposait une notification à l'entité cliente dans des délais non standardisés. La V2.5 aligne les délais sur ceux imposés aux EE par NIS2 : alerte préliminaire dans les 24h, notification intermédiaire dans les 72h, rapport final dans le mois. Ces délais sont désormais opposables contractuellement. Un fournisseur incapable de notifier un incident dans ces délais expose son client EE à un manquement vis-à-vis du CERT-FR, ce qui génère une responsabilité juridique partagée inédite.

La V2.5 impose également la définition préalable d'un canal de notification sécurisé (email chiffré ou portail dédié), testé annuellement dans le cadre d'exercices de gestion de crise.

Authentification forte : généralisation sans exception

La V2.0 recommandait l'authentification multi-facteurs (MFA) sur les systèmes critiques. La V2.5 l'exige pour l'ensemble des accès distants et des accès aux systèmes hébergeant des données classifiées NIS2 ou des actifs critiques identifiés dans la cartographie. Il n'existe plus d'exception sectorielle : y compris pour les PME et ETI, l'absence de MFA sur les accès distants est un écart bloquant en évaluation ReCyF V2.5.

Nouvelles exigences sur la cartographie et la CMDB

La V2.5 introduit une exigence formelle de maintien d'une CMDB (Configuration Management DataBase) à jour pour les actifs critiques, avec une revue documentée au moins semestrielle. Cette exigence, absente de la V2.0, oblige les ETI à formaliser leurs pratiques de gestion des assets, souvent tenues informellement dans des tableurs non versionés.

Impact concret pour les ETI soumises à NIS2 EE/EI

Pour les ETI positionnées comme entités essentielles ou importantes directement, ReCyF V2.5 devient le référentiel d'auto-évaluation recommandé par l'ANSSI pour démontrer la conformité à

l'article 21 de NIS2. Pour les ETI fournisseurs d'EE/EI, ReCyF V2.5 est le questionnaire que leurs clients leur transmettront.

Cartographie des impacts par taille d'entreprise

Les ETI de 250 à 500 collaborateurs disposant d'une DSI structurée peuvent généralement atteindre la conformité V2.5 en 6 à 9 mois avec un accompagnement ciblé. Les points de friction principaux sont la formalisation de la politique fournisseurs, la mise en place du MFA généralisé et la constitution d'une CMDB. Les ETI de moins de 250 personnes avec une DSI réduite ou externalisée font face à un effort plus important, notamment sur la détection (SIEM/SOC) et la gestion des vulnérabilités.

Coûts d'adaptation estimés

Une ETI partant d'un niveau de maturité intermédiaire peut raisonnablement estimer l'effort de mise en conformité ReCyF V2.5 entre 80 000 et 200 000 euros sur 18 mois, incluant les investissements technologiques (MFA, SIEM, outils de gestion des vulnérabilités), la formation des équipes et l'accompagnement par un RSSI externe ou un cabinet spécialisé. Cet investissement est à mettre en regard du risque de perte de contrats : plusieurs EE ont déjà annoncé l'intégration d'une clause de conformité ReCyF dans leurs appels d'offres 2026.

Calendrier d'application et jalons ReCyF V2.5

L'ANSSI a défini un calendrier progressif pour la montée en charge de ReCyF V2.5. Les entités essentielles avaient jusqu'au 1er avril 2026 pour transmettre ReCyF V2.5 à leurs fournisseurs critiques. Les premières évaluations formelles des fournisseurs par les EE sont attendues entre septembre et décembre 2026. Les résultats de ces évaluations alimenteront le bilan annuel de conformité NIS2 que les EE doivent soumettre à l'ANSSI au plus tard le 31 janvier 2027.

Pour les fournisseurs, le calendrier pratique recommandé est le suivant : auto-évaluation initiale avant fin juin 2026, plan de remédiation formalisé en juillet-août, déploiement des mesures prioritaires entre septembre et novembre 2026, évaluation par le client EE en décembre 2026.

Articulation avec MonEspaceNIS2

MonEspaceNIS2, la plateforme de l'ANSSI dédiée à la gestion de la conformité NIS2, intègre depuis avril 2026 un module de suivi ReCyF. Les entités essentielles peuvent y charger les résultats des évaluations de leurs fournisseurs, et les fournisseurs eux-mêmes peuvent partager leurs auto-évaluations directement via la plateforme, facilitant la transmission et la traçabilité des données. Ce module permet également le suivi des plans de remédiation et la génération de tableaux de bord de maturité supply chain.

Domaines ReCyF V2.5 : analyse des 12 domaines

ReCyF V2.5 maintient la structure en 12 domaines de la V2.0, mais redéfinit les niveaux d'exigence attendus. Les domaines les plus impactants pour les ETI fournisseurs sont les suivants :

Domaine 1 : Gouvernance et politique de sécurité

La V2.5 exige non seulement l'existence d'une PSSI (Politique de Sécurité des Systèmes d'Information) mais sa révision documentée annuelle avec validation par la direction générale. La PSSI doit explicitement couvrir les obligations NIS2 applicables et le périmètre des services fournis aux entités NIS2 clientes. Une PSSI générique non actualisée depuis 2023 sera considérée comme un écart majeur.

Domaine 4 : Gestion des actifs

C'est le domaine qui connaît le plus fort renforcement dans la V2.5. La CMDB devient obligatoire (et non plus recommandée) pour les actifs impliqués dans les services fournis aux entités NIS2. La revue d'inventaire semestrielle doit être documentée avec les changements intervenus et les mesures de sécurité associées à chaque asset critique.

Domaine 8 : Gestion des incidents

Aligné sur les nouvelles exigences de notification, ce domaine impose la définition et le test de la procédure de notification des incidents aux entités NIS2 clientes. Le test doit être documenté et les canaux de communication vérifiés annuellement. La désignation d'un point de contact incident nominatif et d'un suppléant est désormais exigée.

Stratégie de mise en conformité ReCyF V2.5 pour les ETI

La mise en conformité ReCyF V2.5 doit être abordée comme un projet structuré, non comme une réponse ad hoc à un questionnaire. Plusieurs approches ont démontré leur efficacité dans les premières démarches conduites en 2025-2026.

Phase 1 : Auto-évaluation et identification des écarts

La première étape est une auto-évaluation honnête sur la grille ReCyF V2.5. Cette évaluation doit mobiliser les responsables métier (IT, RH, juridique, achats) et ne pas se limiter à la DSI. Les contrôles ReCyF couvrent des dimensions organisationnelles et contractuelles qui dépassent largement le périmètre technique. Un RSSI externe peut apporter une neutralité utile à cette phase et identifier des angles morts que les équipes internes auraient tendance à minimiser.

Phase 2 : Priorisation et plan de remédiation

Tous les écarts ne se valent pas. La priorisation doit tenir compte de la visibilité de l'écart lors d'une évaluation client (certains contrôles sont facilement vérifiables, d'autres non), du risque réel qu'il représente, et du coût de remédiation. Le MFA, la CMDB et la procédure de notification d'incidents sont typiquement à traiter en priorité 1, car directement vérifiables et à fort impact perçu par le client EE.

Phase 3 : Déploiement et constitution des preuves

ReCyF V2.5 insiste sur la preuve documentée. Chaque mesure mise en place doit être accompagnée d'une preuve opposable : rapport de déploiement MFA, capture d'écran CMDB avec date, PV de réunion de révision de PSSI avec signature du DG, rapport de test de la procédure d'incident. Ces preuves constituent le dossier de conformité transmis au client EE lors de l'évaluation.

À RETENIR

À retenir

ReCyF V2.5 (mars 2026) renforce 23 contrôles existants, avec une attention particulière sur la supply chain de rang 2, le MFA généralisé et la notification d'incidents harmonisée sur les délais NIS2 (24h/72h/1 mois).

Les ETI fournisseurs d'entités essentielles sont de facto soumises à ReCyF V2.5 via les clauses contractuelles que leurs clients NIS2 sont tenus d'inclure depuis avril 2026.

La CMDB et la politique fournisseurs sont les deux nouveaux points de contrôle les plus structurants de la V2.5, absents ou recommandés dans la V2.0.

MonEspaceNIS2 intègre désormais un module ReCyF permettant aux fournisseurs de partager leurs auto-évaluations directement avec leurs clients EE.

> Le calendrier pratique recommandé : auto-évaluation avant juin 2026, plan de remédiation en juillet-août, déploiement septembre-novembre, évaluation client en décembre 2026.

FAQ : ReCyF V2.5 et impact pour les ETI fournisseurs NIS2

Quelle est la différence entre ReCyF V2.0 et V2.5 pour un fournisseur ?

La V2.5 renforce 23 contrôles existants, notamment sur la gestion de la chaîne d'approvisionnement, l'authentification forte et la notification d'incidents. Pour un fournisseur déjà conforme V2.0, l'effort de mise à niveau est estimé entre 2 et 4 mois de travail, principalement sur la formalisation des preuves et la mise en place de la CMDB.

Mon ETI est-elle obligée de suivre ReCyF V2.5 si elle n'est pas elle-même entité NIS2 ?

Pas directement au sens réglementaire, mais si votre ETI fournit des services à une entité essentielle ou importante, cette dernière est tenue par NIS2 d'inclure des clauses de conformité cyber dans ses contrats. ReCyF V2.5 est le référentiel que la grande majorité des EE françaises utilisent pour formuler ces exigences. Refuser ou ne pas pouvoir répondre à un questionnaire ReCyF expose au risque de perte de contrat.

Quand les premières évaluations formelles ReCyF V2.5 auront-elles lieu ?

Les premières évaluations formelles des fournisseurs par les entités essentielles sont planifiées entre septembre et décembre 2026. Certaines EE des secteurs de l'énergie et des transports ont déjà initié des évaluations pilotes au premier semestre 2026.

ReCyF V2.5 remplace-t-il la certification ISO 27001 ?

Non, ReCyF et ISO 27001 sont complémentaires. Une certification ISO 27001 en cours de validité peut couvrir partiellement les exigences ReCyF, notamment sur les domaines gouvernance, gestion des risques et continuité. Cependant, ReCyF comporte des contrôles spécifiques NIS2 (notification d'incidents, obligations supply chain) que la norme ISO n'adresse pas directement. Un fournisseur certifié ISO 27001 disposera d'un avantage certain mais devra compléter son dispositif pour une conformité complète ReCyF V2.5.

Quelles ressources ANSSI permettent de travailler sur ReCyF V2.5 ?

L'ANSSI met à disposition le guide ReCyF V2.5 complet sur son site cyber.gouv.fr, ainsi que des webinaires de présentation et un service d'accompagnement via MonEspaceNIS2 pour les entités enregistrées. Des prestataires PRIS (Prestataires de Réponse aux Incidents de Sécurité) labellisés proposent également des accompagnements à la mise en conformité ReCyF, avec des durées d'engagement adaptées aux ETI.

Pour approfondir votre démarche de conformité NIS2 supply chain, consultez notre guide complet sur ReCyF et NIS2 supply chain et notre analyse de la directive NIS2 en France. L'ANSSI publie régulièrement des mises à jour sur cyber.gouv.fr, et le texte de référence de NIS2 est consultable sur EUR-Lex. Les fournisseurs du secteur défense doivent également consulter les publications de l'ANSSI relatives au RMC DGA.

ReCyF V2.5 et les prestataires de services numériques : un cas particulier

Les prestataires de services numériques — éditeurs de logiciels, intégrateurs, prestataires cloud, MSSP — occupent une position particulière dans l'écosystème ReCyF V2.5. En tant que fournisseurs quasi-systématiques des entités NIS2, ils sont en première ligne des évaluations ReCyF. Mais ils sont aussi, pour beaucoup d'entre eux, soumis directement à NIS2 en tant qu'entités importantes (prestataires de services cloud, prestataires de services de sécurité gérés sont listés à l'annexe II de NIS2). Cette double position — fournisseur d'EE et EI eux-mêmes —

crée une symétrie réglementaire : ils doivent répondre à ReCyF pour leurs clients EE, tout en devant appliquer l'article 21-4 à leurs propres fournisseurs critiques.

Pour les éditeurs de logiciels fournis aux entités NIS2, ReCyF V2.5 introduit des exigences spécifiques sur la sécurité du cycle de développement (DevSecOps), la gestion des vulnérabilités dans les composants open source (Software Bill of Materials — SBOM), et la procédure de notification des vulnérabilités critiques aux clients. Ces exigences s'alignent avec le Cyber Resilience Act européen, qui entrera progressivement en vigueur entre 2026 et 2028 et imposera des obligations similaires aux éditeurs de logiciels commerciaux.

MSSP et SOC : des obligations renforcées sous ReCyF V2.5

Les Managed Security Service Providers (MSSP) et opérateurs de SOC (Security Operations Center) sont particulièrement ciblés par ReCyF V2.5. En tant que fournisseurs de services de sécurité critiques à des EE, ils bénéficient d'un accès privilégié aux systèmes et aux données de leurs clients. ReCyF V2.5 leur impose les niveaux d'exigence les plus élevés : MFA obligatoire sur tous les accès aux environnements clients, ségrégation logique stricte entre les environnements de différents clients, procédures de notification d'incidents propres à la relation client (distinctes des notifications ANSSI auxquelles ils sont eux-mêmes soumis en tant qu'EI), et audits annuels de sécurité de leurs propres infrastructures de SOC. Un MSSP qui ne peut pas démontrer ces niveaux d'exigence perd rapidement sa crédibilité commerciale auprès des EE, indépendamment de la réglementation.

Retours d'expérience des premières évaluations ReCyF V2.5

Les premières évaluations pilotes menées par des EE des secteurs de l'énergie et des transports au premier semestre 2026 ont mis en évidence des patterns récurrents chez les fournisseurs évalués. Ces retours d'expérience sont précieux pour les fournisseurs qui n'ont pas encore initié leur démarche.

Le constat le plus fréquent est le décalage entre les pratiques réelles et la documentation : de nombreux fournisseurs ont des pratiques de sécurité correctes (MFA déployé, patches appliqués régulièrement, sauvegardes testées) mais n'ont aucune documentation qui le prouve. L'effort de mise en conformité est alors principalement un effort de formalisation et non un effort technique. Ce constat est positif — il signifie que la conformité ReCyF est plus accessible qu'elle n'y paraît pour les entreprises qui ont une culture de la sécurité.

Le deuxième constat est la faiblesse quasi-universelle sur la gestion des sous-traitants : la grande majorité des fournisseurs évalués n'ont aucun processus formel d'évaluation de leurs propres sous-traitants. Or c'est précisément l'exigence renforcée de la V2.5. Ce point représente le chantier le plus structurant pour la plupart des fournisseurs, car il nécessite de sensibiliser et d'embarquer leurs propres fournisseurs dans une démarche cyber.

Le troisième constat est l'hétérogénéité des capacités de réponse selon la taille : les ETI de plus de 250 personnes avec une DSI structurée s'en sortent généralement mieux que les PME de moins de 100 personnes, qui disposent rarement d'un responsable sécurité dédié. Pour ces dernières, un accompagnement externe est quasiment indispensable pour atteindre le niveau "Défini" sur les domaines les plus complexes (gestion des incidents, continuité d'activité).

ReCyF V2.5 dans le contexte européen : vers une harmonisation des référentiels

ReCyF n'existe pas en isolation. Il s'inscrit dans un mouvement européen plus large d'harmonisation des exigences de sécurité de la chaîne d'approvisionnement. L'ENISA a publié en 2025 des lignes directrices sur la sécurité de la supply chain des entités NIS2, qui servent de référence commune aux États membres pour développer leurs propres outils d'évaluation. ReCyF est l'implémentation française de ces lignes directrices, avec des adaptations au contexte réglementaire et sectoriel français.

À l'horizon 2027-2028, une harmonisation européenne des questionnaires fournisseurs NIS2 est attendue, sous l'impulsion de l'ENISA et de la Commission européenne. Cette harmonisation réduira la fragmentation actuelle (chaque pays a son propre référentiel) et permettra aux fournisseurs transfrontaliers de disposer d'un dossier de conformité reconnu dans plusieurs pays.

En attendant, ReCyF reste le standard à maîtriser pour les fournisseurs opérant principalement sur le marché français.

Conclusion : ReCyF V2.5, un investissement stratégique pour les fournisseurs NIS2

La conformité ReCyF V2.5 ne doit pas être perçue comme une contrainte administrative supplémentaire mais comme un investissement stratégique dans la durabilité de la relation commerciale avec les entités NIS2. Les fournisseurs qui anticipent et maîtrisent ReCyF V2.5 acquièrent un avantage concurrentiel réel sur leurs concurrents moins préparés, particulièrement dans les appels d'offres où la conformité supply chain devient un critère de sélection explicite. À moyen terme, la consolidation des référentiels européens et la montée en maturité collective de l'écosystème des fournisseurs NIS2 feront de la conformité ReCyF un standard de marché incontournable, au même titre que la certification ISO 9001 pour la qualité. Les ETI qui construisent dès maintenant leur dispositif de sécurité sur les bases de ReCyF V2.5 se positionnent favorablement pour naviguer les évolutions réglementaires à venir. Pour un accompagnement sur mesure dans votre démarche ReCyF, consultez notre expertise en conformité NIS2 supply chain et notre page dédiée à la directive NIS2. Les ressources officielles ANSSI sont disponibles sur cyber.gouv.fr.