NIS 2 & ReCyF : Les 20 objectifs de sécurité à connaître

Le **Référentiel Cyber France (ReCyF) v2.5** vise à transposer opérationnellement la directive NIS 2 en droit français. Il fixe 20 objectifs de sécurité obligatoires pour les entités importantes (EI) et essentielles (EE), structurés autour de 4 piliers : **Gouvernance, Protection, Défense et Résilience**.

Faites défiler pour découvrir chaque objectif 👇

Infographie réalisée sur la base du
Référentiel Cyber France publié par l'ANSSI

RISKINTEL
MEDIA

STRUCTURE DU RÉFÉRENTIEL

Le ReCyF en un coup d'œil

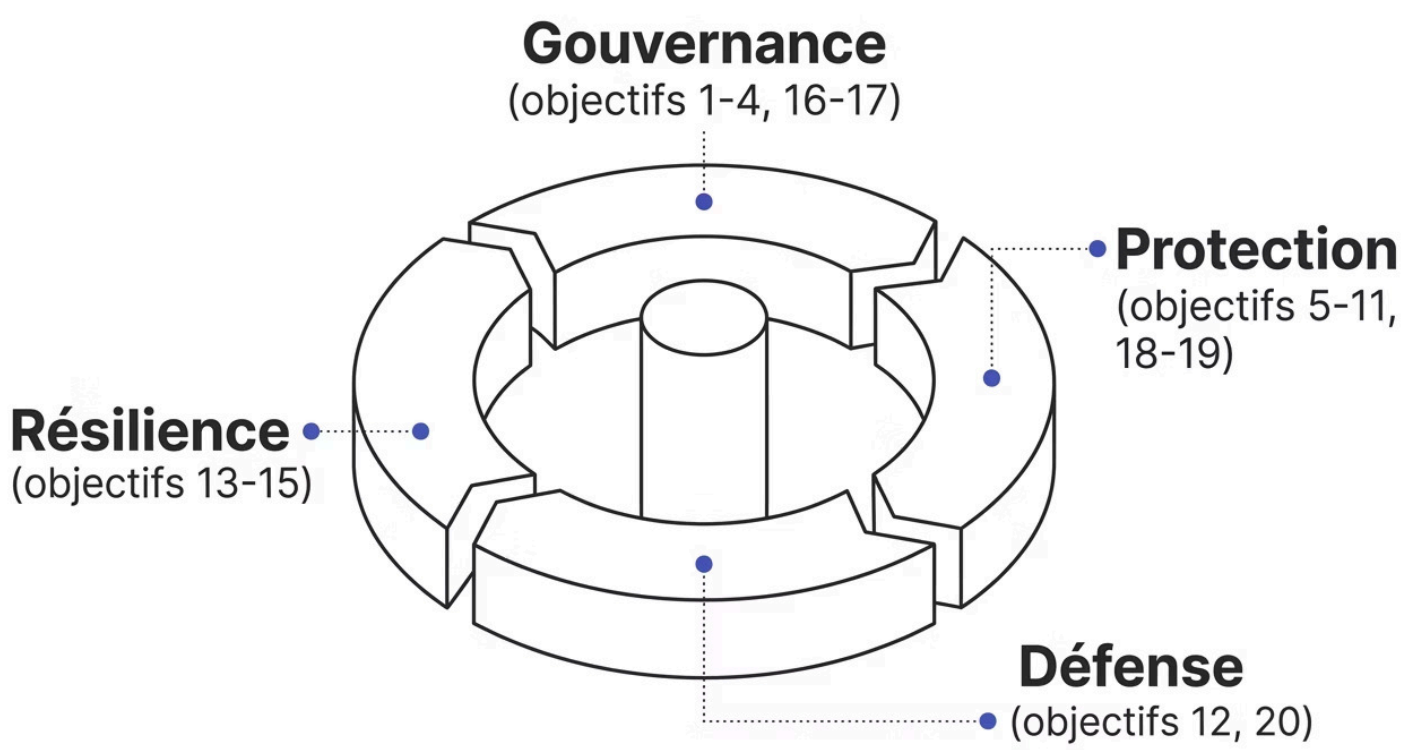
Le référentiel distingue deux types d'obligations et deux catégories d'entités :

Objectif de sécurité

Obligation fixée par décret. Répond à la question **« Quoi ? »**. Application **obligatoire** pour toutes les EI et EE (objectifs 1–15) ou uniquement les EE (objectifs 16–20).

Moyens acceptables de conformité

Mesures proposées par l'ANSSI pour atteindre l'objectif. Répond à la question **« Comment ? »**. Non obligatoires sauf cas particuliers, mais permettent de démontrer la conformité.



GOUVERNANCE — OBJ. 1 & 2

Recensement & Gouvernance des SI

Obj. 1 — Recensement des SI

Lister toutes les activités, services et SI associés. Justifier par analyse de risques les SI exclus du périmètre. Révision annuelle obligatoire. Applicable EI et EE.

Obj. 2 — Cadre de gouvernance

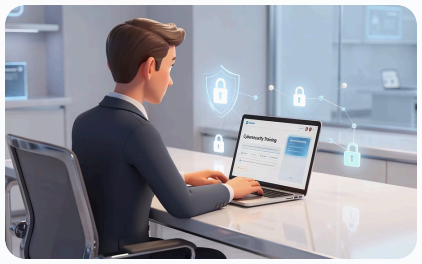
Sous responsabilité du **dirigeant exécutif** : organisation, rôles, PSSI, politiques de chiffrement, contrôle d'accès, gestion des comptes. Plan d'action de conformité obligatoire. Certification **ISO/CEI 27001:2022** acceptée.

GOUVERNANCE — OBJ. 3 & 4

Écosystème & Ressources Humaines

Obj. 3 — Maîtrise de l'écosystème

Cartographier tous les prestataires et fournisseurs informatiques. Intégrer des clauses de sécurité dans les contrats. Vérifier périodiquement la conformité des prestataires. Limiter les risques de compromission par la chaîne de sous-traitance.



Obj. 4 — Intégration RH

Charte d'usage des SI opposable à tous les utilisateurs. Programme de sensibilisation continu. Gestion des arrivées, départs et changements de fonction. Formations dédiées pour les fonctions numériques. Clauses de confidentialité dans les contrats (EE uniquement).

PROTECTION — OBJ. 5 & 6

Maîtrise des SI & Accès Physiques

Obj. 5 — Maîtrise des SI

Cartographie détaillée des SI. Veille sur les vulnérabilités (CERT-FR, CSIRT). Correctifs de sécurité appliqués **sans délai** sur les ressources exposées. Mesures d'atténuation si correctif impossible. Téléchargement depuis sources officielles uniquement.

Obj. 6 — Accès physiques

Contrôle d'accès aux locaux, salles serveurs et locaux techniques. Registre des visiteurs, badges. Vidéosurveillance, gardiennage et alarme (EE). Droits d'accès physiques attribués au strict nécessaire (EE). Personnes externes accompagnées ou autorisées.

PROTECTION — OBJ. 7 & 8

Architecture & Accès Distants

→ Obj. 7 — Sécurisation de l'architecture

Cloisonnement physique et/ou logique des SI (VLAN, VM). Définition de sous-systèmes cohérents (EE). Passerelles entrantes et sortantes dédiées (EE). Filtrage par pare-feu de toutes les communications avec les SI tiers. Revue annuelle des règles de filtrage.

→ Obj. 8 — Accès distants

Chiffrement des accès via SI tiers (VPN TLS/IPSec, SSH). Authentification **multifacteur obligatoire** pour les EE (carte à puce + PIN). Chiffrement des disques des postes mobiles (EE). Mesures d'atténuation si MFA impossible.

PROTECTION — OBJ. 9 & 10

Codes Malveillants & Gestion des Accès

Obj. 9 — Protection contre les codes malveillants

Définir les ressources autorisées à se connecter aux SI. Interdiction du BYOD pour les EE. Antivirus/EDR sur postes, serveurs et équipements mobiles. Analyse systématique des données provenant de sources externes (messagerie, USB, web).

Obj. 10 — Gestion des identités et accès

Comptes individuels pour chaque utilisateur et processus automatique. Désactivation des comptes inutilisés. Authentification avec au moins un élément secret. Droits d'accès attribués au strict nécessaire. Revue annuelle des comptes et des droits.

PROTECTION — OBJ. 11

Maîtrise de l'Administration des SI

L'administration est l'activité la plus ciblée par les attaquants. Un attaquant contrôlant le **cœur de confiance** (annuaires, hyperviseurs, machines d'administration) peut reconstruire entièrement les SI.

01

Comptes dédiés

Comptes d'administration exclusivement réservés aux actions d'administration. Jamais utilisés pour la bureautique quotidienne.

02

Cœur de confiance (EE)

Identifier les ressources constituant le cœur de confiance (annuaires AD, hyperviseurs). Administration depuis des ressources dédiées uniquement.

03

Revue annuelle (EE)

Revue de la configuration des annuaires. Correctifs appliqués sans retard injustifié. Connexions externes au cœur de confiance interdites.

DÉFENSE — OBJ. 12

Identification & Réaction aux Incidents

1

Procédure de traitement (EE)

Élaborer et maintenir à jour une procédure de traitement des incidents. Collecter les signalements des employés, clients et prestataires.

2

Qualification & réaction (EI/EE)

Mécanismes d'analyse et de qualification des événements. Réaction pour limiter les conséquences sur les services. Analyse des causes après chaque incident (EE).

3

Conservation des preuves (EE)

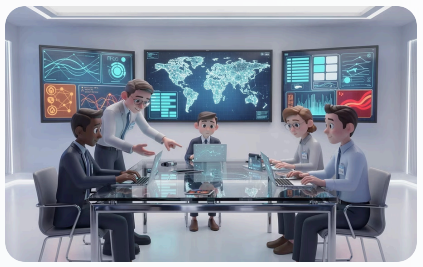
Relevés techniques conservés pour judiciarisation. Stockage hors-ligne pour résister aux rançongiciels. Durée de conservation conforme à la protection des données.

RÉSILIENCE — OBJ. 13 & 14

Continuité, Reprise & Gestion de Crise

Obj. 13 — Continuité & reprise

Procédures de sauvegarde et restauration testées **au minimum une fois par an**. Sauvegardes protégées hors-ligne (anti-rançongiciel). Définir la DMIA et le PRD pour chaque service (EE). PCA et PRA adaptés aux crises cyber (EE).



Obj. 14 — Réaction aux crises cyber

Procédure de gestion de crise cyber documentée. Liste imprimée des personnes mobilisables avec coordonnées. Annuaire des parties prenantes externes. RETEX après chaque exercice ou crise réelle (EE). Stratégie de communication de crise (EE). Moyens de communication de secours (EE).

RÉSILIENCE — OBJ. 15

Exercices, Tests & Entraînements

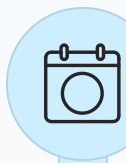
La préparation est clé : des mécanismes non testés peuvent dysfonctionner au moment critique (échec de restauration, bascule sur site de secours).

Exercice sur table (EI/EE)

Au minimum un exercice sur table à fréquence définie par l'entité pour les personnes mobilisables dans la gestion de crise cyber.

Stratégie d'entraînement (EE)

Liste des acteurs, objectifs, scénarios prioritaires, moyens d'évaluation et comitologie de suivi. Tester gestion des alertes, continuité et gestion de crise.



Programme triennal (EE)

Programme sur 3 ans précisant fréquence, nature et objectifs des exercices. Couvrir gestion des incidents, crises cyber et coopération avec l'écosystème.

ENTITÉS ESSENTIELLES UNIQUEMENT

Obj. 16 — Approche par les Risques (EE)

Placée sous la responsabilité du **dirigeant exécutif**, cette approche complète la conformité par une analyse des risques spécifiques à chaque contexte organisationnel et technique.

Gouvernance des risques

Intégrer le risque numérique dans les décisions du dirigeant. Allouer les moyens financiers, humains et techniques adéquats.

Analyse de risques

Chaque SI fait l'objet d'une analyse (méthode EBIOS RM recommandée). S'appuie sur PSSI, cartographie, audits et approche conformité.

Révision triennale

Réexamen au minimum tous les **3 ans** et après tout incident majeur ou évolution du contexte. Acceptation formelle des risques résiduels.

ENTITÉS ESSENTIELLES UNIQUEMENT

Obj. 17 à 20 — Sécurité Avancée (EE)

Obj. 17 — Audit des SI

Programme d'audit planifié selon criticité et exposition. Inclut tests d'intrusion, audits de configuration, d'architecture et organisationnels. Rapport avec constats, vulnérabilités et recommandations. Plan d'action correctif obligatoire. Prestation PASSI qualifiée ANSSI acceptée.

Obj. 18 — Configuration sécurisée

Installer uniquement les logiciels strictement nécessaires. Configurer selon recommandations ANSSI, éditeur ou fabricant. Revue annuelle de configuration (outils automatisés recommandés). Réduire la surface d'attaque des composants SI.

Obj. 19 — Administration dédiée

Postes d'administration dédiés exclusivement à cet usage. Réseau d'administration physiquement ou logiquement cloisonné. Communications d'administration chiffrées et authentifiées. Tunnels VPN si réseau non dédié. Prestation PAMS qualifiée ANSSI acceptée.

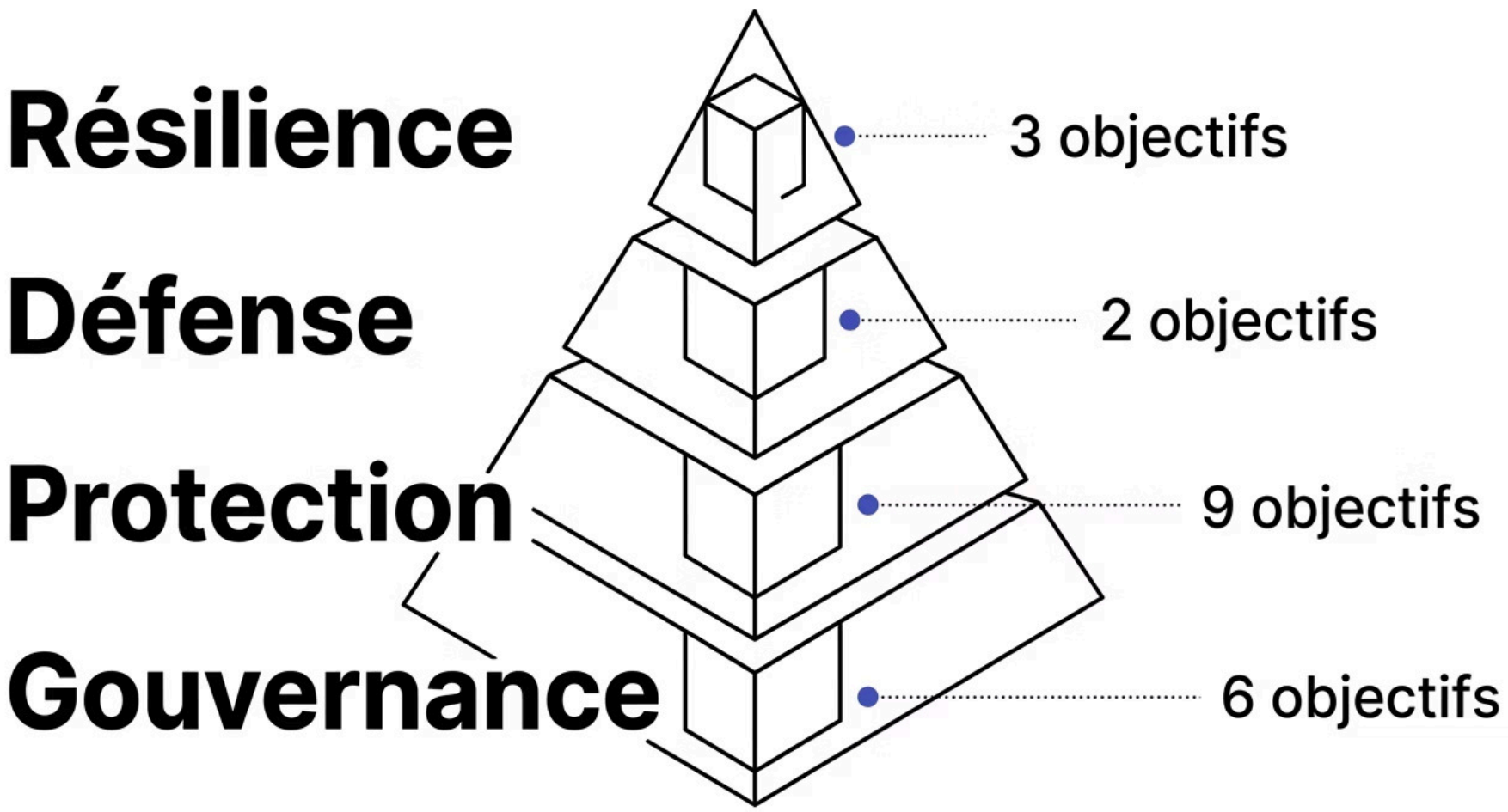
Obj. 20 — Supervision de sécurité

Traitement des journaux et événements de sécurité **sous 24h**. Démarche d'amélioration continue de la supervision. Conservation des événements **au moins 3 mois**. Journaux protégés hors-ligne. Prestation PDIS qualifiée ANSSI acceptée.

TABLEAU DE CORRESPONDANCE

Les 4 Piliers du ReCyF

Les 20 objectifs s'organisent selon le modèle **Gouvernance / Protection / Défense / Résilience** :



CORRESPONDANCE NIS 2

Ancrage dans la Directive NIS 2

Chaque objectif ReCyF correspond à un article de la directive NIS 2. Les principales correspondances :

Art. 20 — Gouvernance

Objectif 2 : approbation et supervision des mesures de cybersécurité par les organes de direction.

Art. 21.2.a — Analyse des risques

Objectifs 2 et 16 : politiques d'analyse des risques et de sécurité des SI.

Art. 21.2.b — Gestion des incidents

Objectifs 12, 15 et 20 : détection, réaction et supervision des incidents.

Art. 21.2.c — Continuité

Objectifs 13, 14 et 15 : sauvegardes, reprise d'activité et gestion des crises.

Art. 21.2.j — Authentification MFA

Objectifs 8, 10, 11 et 14 : authentification multifacteur et communications sécurisées.

Prêt à vous conformer au ReCyF ?

Le ReCyF v2.5 fixe un cadre clair et structuré pour renforcer la cybersécurité des entités importantes et essentielles en France. **15 objectifs** s'appliquent à toutes les EI et EE, **5 objectifs supplémentaires** (16 à 20) sont réservés aux EE.

📌 Partagez ce carrousel

Diffusez ces informations à vos équipes cyber, RSSI et dirigeants concernés par NIS 2.

🔖 Taguez un collègue

Identifiez un responsable sécurité ou un DSI qui doit connaître ces 20 objectifs.

Source : ReCyF v2.5 du 17/03/2026 — ANSSI / Transposition nationale NIS 2 (PJL)

RISKINTEL
MEDIA