

GOUVERNANCE ET SOCLES TECHNOLOGIQUES

Indice de résilience numérique (IRN)

L'Indice de résilience numérique (IRN), lancé en janvier 2026 par aDRI, mesure les dépendances numériques des organisations via 8 piliers et un score de 0 à 100.

Référentiel ou

Cette définition

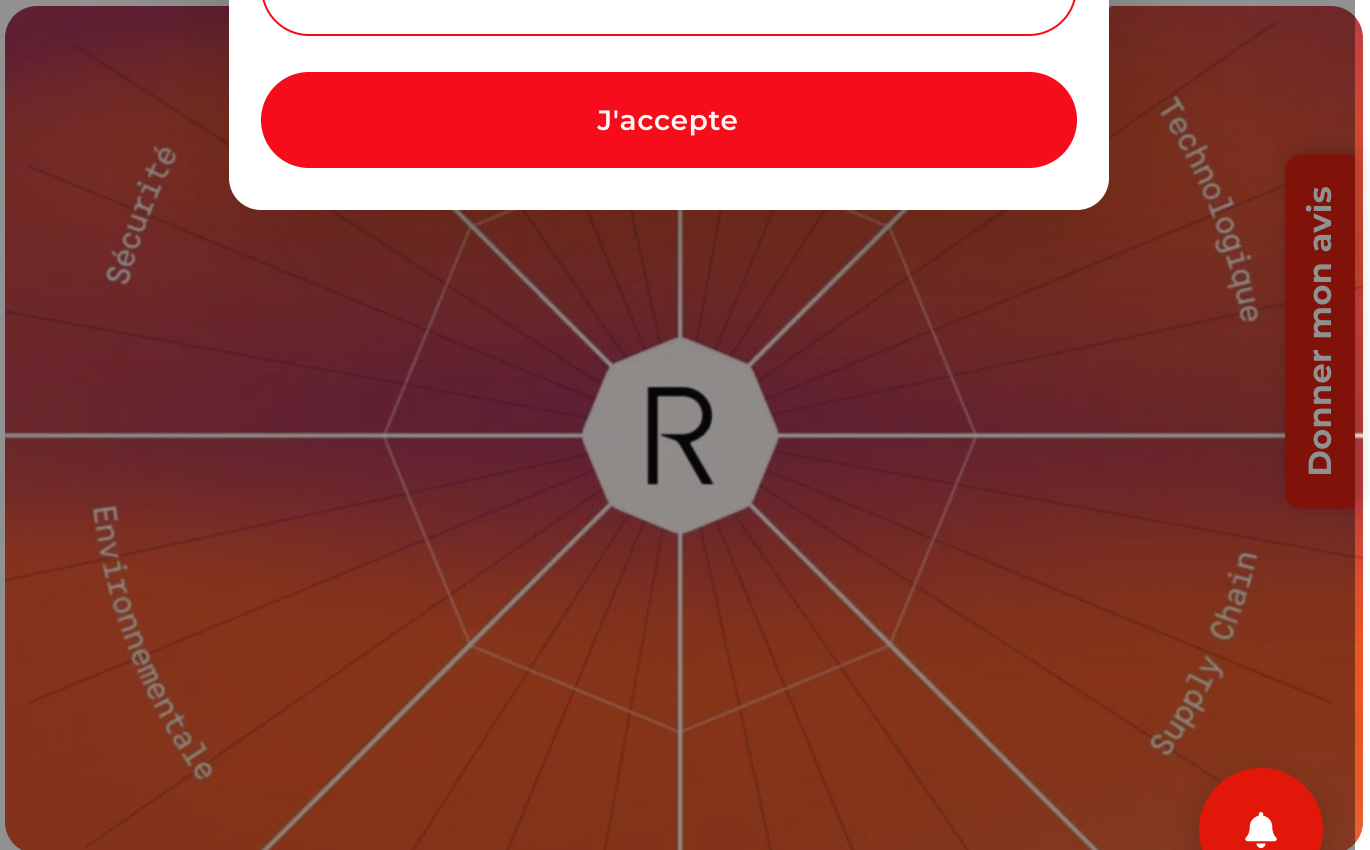
IRN | Digital

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Je refuse

J'accepte

Donner mon avis



L'Indice de résilience numérique (IRN) est un outil de pilotage stratégique permettant aux entreprises, organisations publiques et collectivités territoriales de mesurer, piloter et réduire leurs dépendances numériques critiques.

Il a été officiellement lancé le 26 janvier 2026 à Bercy lors des premières Rencontres de la souveraineté numérique. L'IRN évalue l'ensemble des vulnérabilités d'une organisation sur ses logiciels, données, infrastructures, actifs technologiques, compétences internes, gouvernance et capacité de résilience aux chocs.

L'initiative est portée par l'association à but non lucratif Digital Resilience Initiative (aDRI) en cours de création, cofondée par David Djaïz (Ascend Partners), Yann Lechelle (Sens Digital) et Arno Pons (Digital New Deal), avec Olivier Sichel, Directeur Général de la Caisse des Dépôts, comme Président d'Honneur. aDRI deviendra en 2026 une AISBL (association internationale sans but lucratif) pour accompagner le déploiement européen et international de l'indice.

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Le référentiel est sous licence Creative Commons (CC BY-NC-ND). Il est à disposition pour une auto-évaluation autonome et peut être librement utilisé à condition de prendre la responsabilité de son utilisation. Objectif de l'IRN : renforcer la souveraineté numérique européenne.

La création de l'IRN répond à un constat structurel : le coût de la dépendance numérique de l'Europe est estimé à 265 milliards d'euros selon le CIGREF, avec une grande partie des dépenses des entreprises européennes orientées vers des fournisseurs extra-européens, principalement américains. Dans un contexte marqué par l'intensification des risques géopolitiques, technologiques, industriels et réglementaires, l'IRN ambitionne de donner à l'Europe une boussole concrète pour reconquérir son autonomie numérique.

L'IRN ne promeut pas un repli technologique ou une rupture avec les acteurs américains. Son objectif est de rendre les dépendances visibles, assumées et arbitrables : chaque organisation peut continuer à s'appuyer sur les meilleures technologies disponibles, tout en étant capable de diversifier, migrer, renégocier ou activer des clauses de réversibilité si nécessaire.

Description technique de l'Indice de Résilience Numérique

L'IRN repose sur une méthodologie transparente et ouverte, structurée autour de 8 piliers évaluant la résilience à travers des critères quantitatifs et qualitatifs. Chaque organisation reçoit un scoring de 0 à 100, accompagné de visualisations sous forme de radars visuels (spider charts) et de rapports stratégiques exploitables aussi bien par les COMEX que par les DSI ou les directions des risques.

Les 8 piliers de l'IRN

- Résilience stratégique
- Résilience économique et juridique
- Résilience data et IA
- Résilience
- Résilience
- Résilience
- Résilience
- Résilience

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Méthodologie

L'évaluation s'appuie sur :

- **Critères quantitatifs** - Ils mesurent factuellement l'indépendance du système d'information, à trois échelles (nationale, européenne, extra-européenne).
- **Critères qualitatifs** - Ils évaluent la culture et l'organisation de l'entreprise vis-à-vis de ces enjeux.

Chaque critère reçoit un score R (Résilient) ou NR (Non Résilient), agrégé dans un score global de 0 à 100. L'approche part non pas de l'inventaire technique des systèmes, mais des métiers vitaux de chaque organisation : à partir des fonctions critiques, l'outil reconstruit les systèmes numériques qui les soutiennent et les évalue.

Cadre réglementaire et juridique lié à l'IRN

L'Indice de résilience numérique s'aligne étroitement sur les réglementations européennes structurantes en matière de numérique, de cybersécurité et de protection des données.

Directive NIS2

L'IRN évalue la capacité technique, organisationnelle et contractuelle d'une organisation à garantir la continuité des services essentiels, en s'appuyant sur des critères tels que la redondance des dispositifs, l'analyse des risques fournisseurs, la localisation souveraine des données et la robustesse des plans de continuité. Dans la chaîne d'approvisionnement numérique, l'IRN oriente la rédaction des clauses contractuelles relatives aux fournisseurs tiers, sous l'aspect direct et indirect.

Souhaitez-vous recevoir nos notifications de nouveaux articles ?

RGPD et protection des données

L'indice intègre les exigences de la réglementation européenne en ce qui concerne la localisation des données de l'Union européenne, la protection des données sensibles et les mesures de sécurité appliquées aux données.

Règlement DORA

Le règlement européen sur la résilience opérationnelle numérique du secteur financier (DORA) partage une logique similaire à celle de l'IRN. L'indice s'inspire de cette approche en évaluant la résilience opérationnelle à partir des systèmes critiques de chaque organisation, quel que soit son secteur d'activité.

AI Act et Data Act

L'IRN prend en compte les exigences de l'AI Act en matière de gouvernance des systèmes d'intelligence artificielle (traçabilité, supervision humaine, conformité des

données d'entraînement) et celles du Data Act sur la gouvernance et le partage des données.

Complémentarité avec les audits ANSSI

En miroir des audits de conformité menés par l'ANSSI, l'IRN dévoile les angles morts du système d'information, privilégiant une vision transversale indispensable au pilotage de la sécurité. L'indice encourage l'intégration de politiques documentées : procédures de gestion d'incidents, traçabilité des vulnérabilités, formation des agents et adoption de solutions certifiées. L'IRN devient ainsi une pièce à verser au dossier lors de la démonstration, auprès des financeurs ou des autorités, du sérieux d'une démarche en cybersécurité.

Enjeux de l'IRN pour développer la cybersécurité

Pour les collectivités, l'IRN est un outil précieux dans un contexte où la cybersécurité a un impact sur ce qui compte : la continuité de l'activité. L'IRN est une boussole pour la cybersécurité. **IA et Cybersécurité** : les enjeux de la convergence des technologies et des enjeux de la cybersécurité. L'IRN offre une grille de lecture transversale pour piloter l'ensemble de ces conformités de manière cohérente.

Souhaitez-vous recevoir nos notifications de nouveaux articles ?

Une boussole pour la cybersécurité

L'IRN est un outil précieux dans un contexte où la cybersécurité a déjà un impact sur ce qui compte : la continuité de l'activité. L'IRN est une boussole pour la cybersécurité. **Concurrence Data**, les enjeux de la convergence des technologies et des enjeux de la cybersécurité. L'IRN offre une grille de lecture transversale pour piloter l'ensemble de ces conformités de manière cohérente.

Réglementation applicable aux collectivités

Les collectivités sont directement concernées par plusieurs des réglementations intégrées dans l'IRN. Le RGPD impose une protection stricte des données personnelles des citoyens. La directive NIS2 étend ses obligations à de nombreuses entités publiques. Les **précautions juridiques liées à l'IA générative** (AI Act, Data Act, RGS) s'ajoutent à ce cadre. L'IRN offre une grille de lecture transversale pour piloter l'ensemble de ces conformités de manière cohérente.

Acteurs et déploiement

Alliance public-privé

Le lancement de l'IRN a été officialisé le 26 janvier 2026 à Bercy avec le soutien ministériel de Madame la Ministre déléguée Anne Le Hénanff, en présence du CIGREF et de Numeum, les deux principales organisations professionnelles du numérique en France.

Partenaires fondateurs et design partners

Les premières organisations ayant expérimenté l'IRN en tant que « design partners » sont issues de secteurs variés, démontrant l'universalité de l'outil :

- RTE
- Docapost
- Caisse de
- CMA-CGM
- MAIF
- SNCF
- Groupe A
- Orange
- Ouest-France

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

- Description technique de l'Indice de Résilience Numérique
- Les 8 piliers de l'IRN
- Méthodologie d'évaluation
- Cadre réglementaire et juridique lié à l'IRN
- Directive NIS2

- RGPD et protection des données
- Règlement DORA
- AI Act et Data Act
- Complémentarité avec les audits ANSSI
- Enjeux de l'IRN pour les collectivités territoriales : une boussole pour développer la souveraineté numérique et la cybersécurité
- Réglementation applicable aux collectivités
- Acteurs et
- Alliance p
- **Partenair**

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Cette définition vous a été utile ?

 **Oui**

 **Non**

Questions fréquemment associées à Indice

de résilience numérique (IRN)

Comment l'IRN mesure-t-il la dépendance aux fournisseurs de logiciels étrangers ?



L'IRN comptabilise la part des dépenses consacrées aux logiciels et licences issus de fournisseurs non européens, tout en distinguant les investissements vers le national ou l'europpéen. Il interroge ensuite la géolocalisation du stockage des données, identifiant celles hébergées hors d'Europe. Au-delà de ces critères quantitatifs, l'indice évalue la capacité de l'organisation à migrer entre fournisseurs, l'existence de clauses de réversibilité contractuelles et le degré d'appui sur des technologies ouvertes (open source, standards ouverts) qui réduisent le risque de vendor lock-in.

Qui est à l'origine de l'IRN ?

L'IRN a été initié par le think tank Digital Resilience Initiative, présidé par Jean-François Lelièvre. L'initiative est financée par le GREF, Numeum, et bénéficie d'un soutien technique de la part de la Direction Générale de la Résilience (DGR).

Souhaitez-vous recevoir nos notifications de nouveaux articles ?



(al) et Arno Pons
al Resilience
e des Dépôts.
GREF, Numeum,

Quels sont les 8 piliers de l'IRN ?



L'IRN structure son évaluation autour de 8 piliers : résilience stratégique (vision tech, gouvernance IT), résilience économique et juridique (conformité RGPD, AI Act, NIS2), résilience data et IA, résilience opérationnelle (continuité d'activité), résilience supply-chain (diversification fournisseurs), résilience technologique (open source, cloud souverain), résilience sécurité (cybersécurité) et résilience environnementale (Green IT, sobriété numérique).

L'IRN est-il obligatoire pour les collectivités territoriales ?



Non, l'IRN repose sur une démarche volontaire. Aucune obligation réglementaire n'impose son utilisation. Cependant, pour les collectivités soumises à la directive NIS2, au RGPD ou devant démontrer la robustesse de leur cybersécurité auprès de financeurs, l'IRN constitue un outil précieux de pilotage et de preuve de maturité numérique. La note obtenue peut faciliter l'accès à des financements dédiés à la cybersécurité ou à la transition vers des clouds souverains.

Quel est le lien entre l'IRN et les réglementations NIS2, RGPD, DORA et AI Act ?



L'IRN s'aligne sur les exigences de conformité au RGPD (protection des données personnelles), à la directive NIS2 (sécurité des systèmes d'information), au Data Act (gouvernance des données) et à la réglementation sur l'IA (intelligence artificielle).

Souhaitez-vous recevoir nos notifications de nouveaux articles ?

Il évalue la conformité des systèmes d'information, du traitement des données (protection), de la résilience numérique (sécurité) et du respect des principes éthiques (intelligence artificielle) et du respect des principes de gouvernance.

L'IRN est-il gratuit ?



Oui. Le référentiel méthodologique est publié sous licence Creative Commons (CC BY-NC-ND), ce qui signifie que toute organisation peut l'utiliser gratuitement pour réaliser une auto-évaluation de ses systèmes critiques. Pour les organisations souhaitant un accompagnement certifié, des cabinets d'audit agréés par aDRI pourront à terme labelliser les évaluations.

Quelle différence entre résilience numérique et souveraineté numérique ?



La souveraineté numérique relève du domaine régalien : elle désigne la capacité d'un État à exercer un contrôle sur ses données, ses infrastructures et son espace numérique. La

résilience numérique est une notion opérationnelle, à l'échelle de l'entreprise ou de la collectivité : elle mesure la capacité d'une organisation à fonctionner, résister et se rétablir face à un choc ou une défaillance de ses systèmes numériques. L'IRN mesure la résilience, qui contribue à renforcer la souveraineté sans s'y substituer.

Qu'est-ce que le Baromètre de Souveraineté Numérique (BSN) ?



Le BSN est le pendant macroéconomique de l'IRN. Alors que l'IRN fournit un diagnostic individuel par organisation, le BSN agrège les données pour mesurer la dépendance numérique secteur par secteur, à l'échelle nationale. Il alimentera les travaux de l'Observatoire de la souveraineté numérique, permettant d'orienter les politiques publiques et les investissements stratégiques.

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Ressources externes associées à Indice de résilience numérique (IRN)



Site de l'association Digital Resilience Initiative : méthodologie complète, référentiel, actualités et démarche d'auto-évaluation.

Site officiel aDRI

Je découvre

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

DIRECT_NUMERIQUE



er le défilement

Les termes en lien avec Indice de résilience numérique (IRN)

CLOUD Act

Le CLOUD Act américain est une loi extraterritoriale adoptée en 2018 qui permet aux autorités américaines d'accéder à des données détenues par des fournisseurs soumis au droit américain, même lorsqu'elles sont hébergées hors des États-Unis. Pour les collectivités françaises, ce texte soulève des enjeux majeurs de souveraineté numérique et de protection des données des habitants. Comprendre ses implications concrètes est essentiel pour sécuriser...

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

[Lire la définition](#)

Sobriété numérique

La sobriété numérique est une démarche visant à réduire l'impact environnemental du numérique.

[Lire la définition >](#)

Souveraineté numérique

Dans un contexte de tensions géopolitiques et de dépendances technologiques croissantes, la souveraineté numérique désigne la capacité d'un État ou d'une organisation à maîtriser ses nouvelles technologies, ses données et ses infrastructures numériques. Pour les collectivités, cette maîtrise n'est plus une option mais une nécessité pour garantir la continuité du service public. Cet article vous propose une définition accessible, une approche technique, une...

[Lire la définition](#) >

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Les propositions en lien avec Indice de résilience numérique (IRN)

GOVERNANCE ET SOCLES TECHNOLOGIQUES

Réduire les impacts environnementaux de son système d'information pour renforcer sa conformité réglementaire

Souhaitez-vous recevoir nos notifications de nouveaux articles ?

TRANSITION

Utiliser l'IA pour améliorer la performance de son système d'information numérique

Je découvre

GOVERNANCE ET SOCLES TECHNOLOGIQUES

Héberger ses données à l'abri des lois extraterritoriales

[Je découvre](#)

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Les retours d'expérience en lien avec Indice de résilience numérique (IRN)



Michel Ballereau

Une offre de
Essonne N

GOVERNANCE

**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

en place par



Cyrille Barrières, Ville de Châlons-en-Champagne

Châlons-en-Champagne (51) construit son projet autour d'un hyperviseur souverain open source

GOVERNANCE ET SOCLES TECHNOLOGIQUES

[Je découvre](#)



**Souhaitez-vous recevoir nos notifications
de nouveaux articles ?**

Bertrand Maes,

La Ville de
construit u

ATTRACTIVITÉ E

érique et
tétaires

[Je découvre](#)