



DOCAPOSTE

La maîtrise de votre avenir numérique commence par la mesure de votre résilience

par Julie TISSERAND & François BERAT

L'enjeu de résilience des SI des collectivités est majeur puisqu'il impacte directement la continuité du service public

Les intervenants



François BERAT
Directeur Conseil Secteur Public
francois.berat@softeam.fr



Julie TISSERAND
Directrice des Offres
julie.tisserand@softeam.fr

Des services publics de + en + digitalisés...

Les collectivités ont largement **digitalisé leurs activités et leurs relations aux usagers** :

- Logique de plateforme de services publics numériques
- Accélérés par les doctrines de l'état (Ex. Cloud au centre / état plateforme)
- Et les attentes des citoyens

...dans un contexte opérationnel exigeant



Par nature, les collectivités exercent une forte diversité des métiers, sont présentes sur de nombreux sites et doivent absorber de nouvelles politiques publiques et réglementations

→ Nombreux composants et solutions / éditeurs, complexité infrastructures (réseau / téléphonie)...



Des dépenses SI devenues obligatoires dans un cadre budgétaire contraint

→ Récurrences des coûts des services, augmentation du patrimoine applicatif, inflation des coûts éditeurs



Contraintes de la commande publique

→ Un peu moins d'agilité, projets plus longs

Une couverture partielle de la notion de résilience numérique



Définition retenue → Capacité à résister à une perturbation majeure de ses services numériques, qu'elle soit d'origine technique, juridique, géopolitique, économique ou environnementale

DÉPENDANCE AUX FOURNISSEURS TECHNOLOGIQUES

Dépendance à des acteurs dominants, le + souvent extra-européens : Microsoft, VMWare, hyperscalers ...

→ **Met en risque la résilience économique, juridique et géopolitique**

RÉVERSIBILITÉ & VENDOR LOCK-IN

Incapacité à migrer vers une alternative dans des délais maîtrisés

→ **Met en risque l'autonomie économique, contractuelle et stratégique face à ses fournisseurs**

DISPONIBILITÉ DES COMPÉTENCES

Dépendance à un nombre réduit d'agents ou prestataires détenant les compétences clés

→ **Met en risque la capacité à opérer les services + à gérer une crise**

OBSOLESCENCE TECHNOLOGIQUE

Maintien en production de composants en fin de support, faute de budget ou de priorité politique

→ **Met en risque la sécurité et la pérennité des services numériques**

GOVERNANCE DES USAGES I.A.

Adoption spontanée d'outils IA grand public par les agents, sans politique ni traçabilité

→ **Met en risque la conformité et la souveraineté des données des administrés**

ALÉAS ENVIRONNEMENTAUX

Absence d'intégration des risques climatiques et énergétiques dans la continuité des SI

→ **Met en risque disponibilité des services publics en cas de sinistre**

C'est quoi l'Indice de Résilience Numérique ?



PROBLÉMATIQUE À LAQUELLE IL RÉPOND

Mesurer objectivement sa capacité à résister à une perturbation majeure de ses services numériques, qu'elle soit d'origine technique, juridique, géopolitique, économique ou environnementale



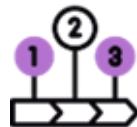
LA FINALITÉ

- Pour le **COMEX** : indicateur synthétique et radar visuel permettant d'arbitrer les investissements de résilience au bon niveau, avec des données factuelles plutôt qu'un ressenti
- Pour les **directions opérationnelles** : grille d'évaluation structurée qui révèle les angles morts et souligne les mesures à prendre



D'OÙ IL VIENT

- Construit par l'aDRI⁽¹⁾ et un écosystème de « Design Partners » privés et publics, parmi lesquels RTE, Crédit Mutuel, la Caisse des Dépôts et Docaposte
- Commun d'intérêt général pour évaluer le niveau de résilience numérique d'un système / d'une fonction dans l'objectif de le sécuriser



COMMENT IL SE DÉPLOIE

- S'applique à une fonction / un système (critique en priorité)
- 8 piliers de résilience dont les critères sont évalués de 0 à 5 : résilience stratégique, économique et juridique, data & IA, opérationnelle, supply chain, technologique, sécurité et environnementale
- Analyse à l'échelle des composants et réagréé à l'échelle des applications et/ou des fonctions

Les critères derrière l'IRN



RES-1 | Résilience Stratégique

Vision tech & Roadmap

Gouvernance IT

Gouvernance usages



RES-2 | Résilience Economique & Juridique

Conformité réglementaire

Audit & Certification

Souveraineté juridique

Stratégie d'indépendance



RES-3 | Résilience Data & IA

Contrôle des données

Infrastructure IA

Éthique & Transparence



RES-4 | Résilience Opérationnelle

Continuité d'activité

Gestion des incidents

Plans de reprise



RES-5 | Résilience Supply-Chain

Fournisseurs critiques

Diversification

Contrats & SLA

Transparence



RES-6 | Résilience Technologique

Infrastructure & Cloud

Application & SaaS

Open-source

Gestion obsolescence



RES-7 | Sécurité & Résilience

Cybersécurité

Protection des données

Gestion des risques

Pilotage logs



RES-8 | Résilience Environnementale & énergétique

Empreinte carbone

Green IT

Durabilité numérique

Dépendance énergétique

Le déploiement du diagnostic au sein d'une organisation

ÉTAPE N° 1 | PILOTE



Définition d'un périmètre pilote

- Système(s) au cœur de **processus métiers critiques** pour la structure
- Système(s) au cœur d'une fonction ayant une **sensibilité / visibilité politique**
- Système(s) dont le périmètre est **régulé**
- Système(s) bien **documenté(s)**



Choix d'un modèle organisationnel

- **Modèle concentré** avec la mise en place d'une équipe-cœur client composée de 3 à 5 interlocuteurs pluridisciplinaires
- **Modèle déconcentré** avec l'implication de toutes les parties prenantes concernées par les critères de l'IRN, notamment au travers d'ateliers thématiques



Déploiement & Apprentissage

- Déploiement de l'évaluation sur le périmètre pilote défini
- Sensibilisation des équipes impliquées en fonction du modèle organisationnel sélectionné
- Gabarisation du déploiement de l'évaluation pour l'extrapoler à l'échelle de toutes les fonctions critiques



ÉTAPE N° 2 | PASSAGE À L'ÉCHELLE

- Cartographie complète des composants des périmètres définis comme critiques
- Déploiement de l'évaluation et production d'analyses à l'échelle des fonctions identifiées



ÉTAPE N° 2B ou 3 | REMÉDIATION

- Construction d'une feuille de route de remédiation de la dette de résilience mesurée
- Priorisation & Mise en place des recommandations prioritaires

Comment ça marche ?

Focus sur la méthode de déploiement d'un diagnostic pilote

1

CADRAGE

Définition du périmètre du diagnostic de résilience et des parties prenantes à impliquer

Définition du périmètre pilote

Planification du diagnostic

2a

CARTOGRAPHIE

Cartographie technico-fonctionnelle de chaque périmètre pilote avec les composants et adhérences

Macro-cartographie du périmètre

2b

QUALIFICATION

Évaluation des composants avec la qualification de sous-critères de résilience déduits de l'IRN

Composants qualifiés

2c

AGRÉGATION

Réagrégation des évaluations des composants à l'échelle des applications et des fonctions via l'algorithme de l'aDRI

Évaluation de la résilience

3

RESTITUTION

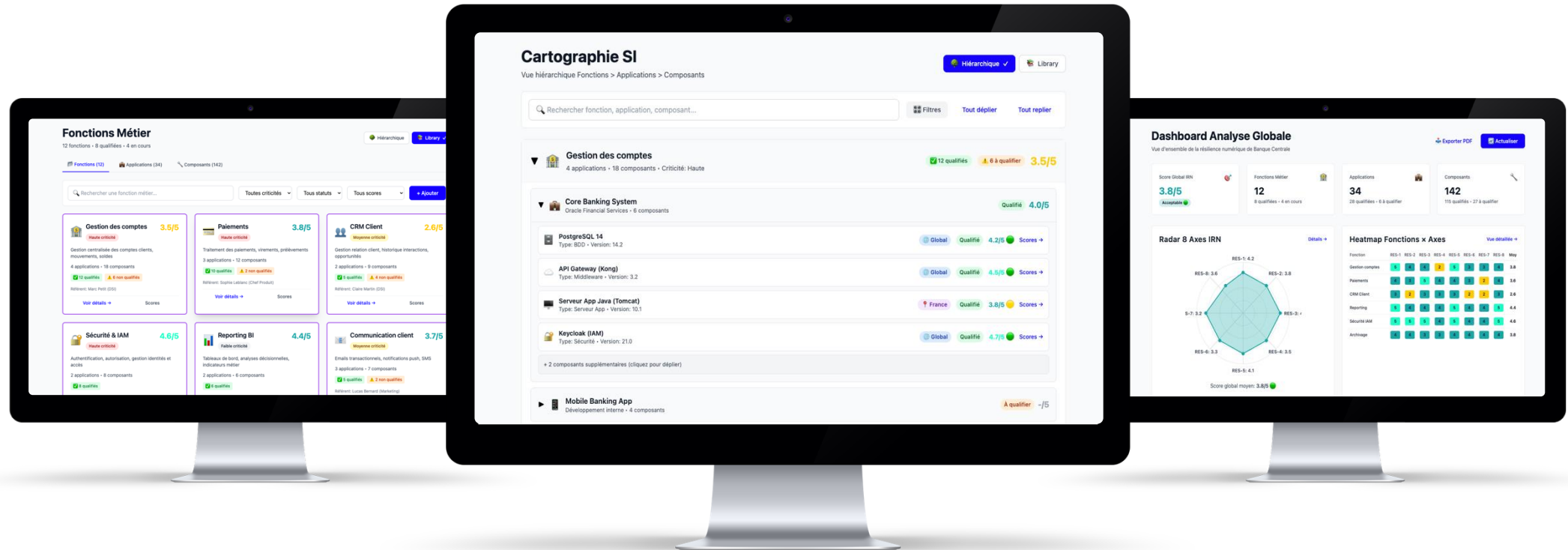
Présentation du niveau de résilience évalué, gabarisation du déploiement sur le périmètre pilote pour extrapoler un passage à l'échelle

Synthèse des résultats du diagnostic

Recommandations majeures

Exemples de vue d'analyses

Extrapolation sur la base des données collectées lors du déploiement



Construire & Déployer les plans de transition vers plus de résilience numérique par une approche modulaire

Gouvernance

- Doctrine de résilience
- Plan d'acculturation
- Adaptation de la gouvernance (résilience, data, IA, ...)
- Mise en place de tableaux de bords et KPIs

Feuille de route

- Mise en place d'une feuille de route dédiée ou intégration d'un pan de résilience à la feuille de route SI
- Priorisation & Analyse d'impacts
- Modélisation
- Pilotage de la feuille de route / de programmes et projets associés

Solutions

Études & Aide au choix

- Études d'architecture
- Stratégie make or buy
- Sourcing de solutions alternatives
- Benchmark de solutions résilientes et opensource
- Accompagnement sur les procédures d'achats (RFI / RFP)

Déploiement

- Plan de déploiement
- Tests / Expérimentations
- Pilotage & Communication
- Conduite du changement

Opérationnalisation

Évolution des processus

- Adaptation des processus Achats : contrats et clauses, évolution des critères de notation des AOs, multi-sourcing, ...
- Adaptation des processus RH : GPEC, ...

Procédures opérationnelles

- Déploiement de PCA / PRA
- Intégration des aléas environnementaux
- Définition et tests des niveaux de services

Notre positionnement sur les enjeux de résilience



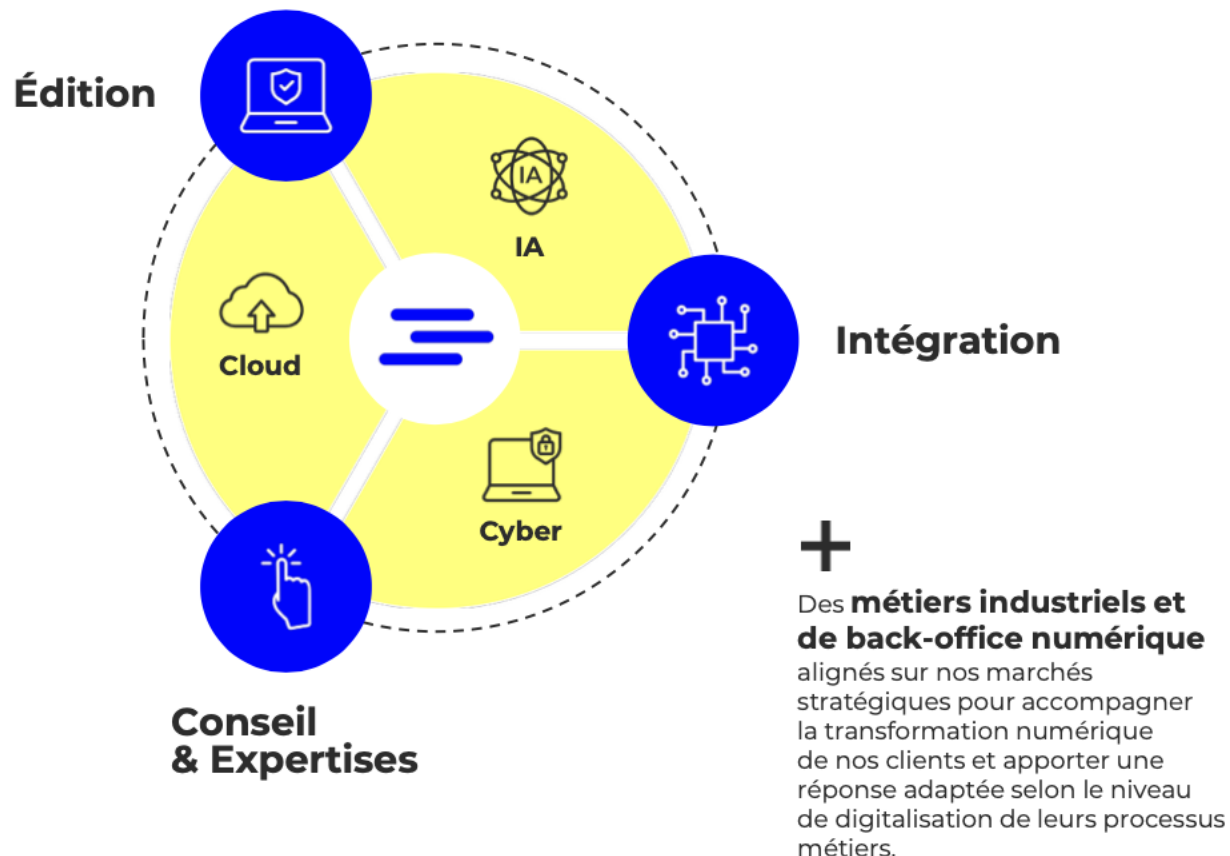
La **Caisse des Dépôts**, tiers de confiance de l'État depuis 1816, étend sa mission de protection de l'intérêt général au numérique : investissement dans le cloud souverain (NumSpot via la Banque des Territoires), soutien à l'identité numérique, inclusion numérique des territoires et financement de l'écosystème tech français. Ce positionnement fait de la CDC l'architecte institutionnel d'une souveraineté numérique à la française, articulant acteurs publics et privés pour construire des alternatives crédibles aux hyperscalers.



Docaposte, filiale numérique du groupe La Poste, est le principal opérateur français de services de confiance numérique : identité numérique (La Poste Identité Numérique), signature électronique, archivage à valeur probante, hébergement de données de santé (HDS), et chef de file du cloud souverain NumSpot. En développant sa propre ferme GPU et un orchestrateur d'agents IA souverain, Docaposte remonte la chaîne de valeur pour offrir une alternative maîtrisée sur l'ensemble de la stack — de l'infrastructure au traitement intelligent des données.

Le groupe Caisse des Dépôts apporte la légitimité institutionnelle (Olivier Sichel préside l'aDRI) et ancre l'IRN comme un commun d'intérêt général, tandis que Docaposte, en tant qu'entreprise pilote et acteur du cloud de confiance, se positionne à la fois comme co-constructeur du référentiel et comme partenaire d'accompagnement pour transformer le diagnostic en trajectoire de résilience concrète — passant ainsi du thermomètre au traitement.

Nos métiers et savoir-faire technologiques au service de nos marchés stratégiques



Santé

Solutions logicielles Métier
Plateformes digitales et humaines
Conseil & Expertises

49 millions de dossiers
pharmaceutiques

**IA générative éthique et
souveraine** DALVIA Santé

3 millions de flux de facturation /
jour / messagerie sécurisée pour
l'Assurance Maladie



Secteur Public

Solutions et plateformes
pour la digitalisation des entités
publiques et parapubliques

5 millions d'avis Droit au
logement

3,5 millions Comptes Personnels
de Formation sécurisés

18 millions
d'utilisateurs PRONOTE



Finance

Digitalisation et conformité des
parcours client, lutte contre la fraude,
valorisation des données financières,
transition durable

23 000 sinistres catastrophes
naturelles et sécheresse

141 millions de déclarations
véhicules assurés

+ 500 000 clients bancaires
personnes physiques remédiées KYC



Autres secteurs

Digitalisation et optimisation des
processus métiers et de l'expérience
utilisateur

+ de 23 000
comptes
facturés

Près de 180 millions
de factures
dématérialisées

L'Offre Conseil & Services de Docaposte

Un accompagnement pour chaque dimension de votre transformation

Transformation digitale

- Stratégie digitale
- Web & Social Media
- Nouveaux usages

Transformation data et IA

- Gouvernance de la donnée
- IA pour la DSI / IA pour les métiers
- Big Data

Transformation SI

- Transformation & Stratégie SI
- Architecture & Urbanisation SI
- Cloud & Hybridation

Transformation métier

- ESG
- Organisation & processus
- Pilotage de la transformation

Transformation réglementaire

- Risk Management
- Mise en conformité
- Cybersécurité

Et une gamme complète pour accompagner l'amélioration de votre résilience

Évaluation du niveau de résilience numérique des fonctions critiques d'une organisation & Pilotage opérationnel de la résilience sur la durée

Substitution des solutions extra-européennes par l'**intégration d'alternatives souveraines** (FR ou EU)

Hybridation Cloud avec des fournisseurs européens pour réduire la dépendance aux hyperscalers progressivement

Mise en œuvre d'une gouvernance de la donnée pour accentuer la maîtrise opérationnelle de ses données et maximiser la valeur générée

Formation au numérique de confiance pour réduire la dépendance aux compétences individuelles et encadrer les usages

Mise en conformité avec le cadre normatif cyber (NIS2, LPM) pour l'utiliser comme levier de résilience opérationnelle réelle pour les SI

Conception et urbanisation du SI pour réduire les dépendances critiques et planifier la modernisation du SI avec une résilience dès la conception



DES QUESTIONS ?