Livre blanc

Cloud souverain

maîtriser les risques à l'heure des tensions numériques mondiales

SiGMA
NUMÉRIQUE À IMPACT

SOMMAIRE

CLOUD SOUVERAIN : MAÎTRISER LES RISQUES À L'HEURE DES TENSIONS NUMÉRIQUES MONDIALES

En 2025, plus de 60 % des dépenses IT mondiales sont orientées vers des services cloud[1], traduisant une bascule massive vers des architectures agiles, scalables et externalisées. Le cloud représente une brique essentielle de la compétitivité et de la continuité d'activité.

Cette transformation rapide, accélérée depuis la crise sanitaire de 2020, s'est heurtée à un nouveau mur : celui de la souveraineté numérique. En France, 67 % des dirigeants interrogés déclarent que la localisation des données et le respect des réglementations européennes sont devenus des critères décisifs dans leurs choix de fournisseurs cloud[2].

Et pour cause : la menace est bien réelle. Les départements IT doivent composer avec :

- Un cadre réglementaire de plus en plus exigeant
- Des technologies toujours plus sophistiquées
- Des risques extraterritoriaux croissants, incarnés par des lois comme le Cloud Act ou le Foreign Intelligence Surveillance Act (FISA) aux États-Unis
- La montée des tensions géopolitiques qui ravivent les craintes d'espionnage industriel ou de perte de souveraineté sur les données critiques : plus de 40 % des entreprises considèrent la protection des données comme un enjeu très important dans le cloud[3].

Dans ce contexte, comment tirer parti du cloud sans céder sur la sécurité, la conformité et le contrôle ?

Comment faire du cloud un **levier de progrès durable**, fondé sur la confiance, la responsabilité et la maîtrise ?

[1] Gartner, Forecast: Public Cloud Services Worldwide, 2024.
[2] IDC, France Cloud Survey, 2024 : enquête sur les critères de choix cloud.
[3] Etude Markess Exaegis "Cloud de confiance : où en est-on en 2025 En France ?"

EDITO

Chez Sigma, notre engagement en tant qu'entreprise à mission repose sur une conviction forte : le numérique doit être un levier de progrès durable et de confiance. Faire confiance, c'est accepter de confier quelque chose de précieux — ses données, ses infrastructures, sa stratégie numérique — à un partenaire digne de cette responsabilité. C'est aussi attendre en retour de la crédibilité, de la sécurité et de la loyauté.

Dans un environnement numérique traversé par des risques réglementaires, technologiques et géopolitiques croissants, cette confiance devient un actif stratégique pour les DSI, RSSI, responsables d'infrastructure et directions générales. Elle ne se décrète pas : elle se construit. Dans la durée. Par la proximité, l'excellence opérationnelle, la transparence, la résilience, mais aussi par une maîtrise souveraine des données et dans le respect des réglementations qui contrôlent le secteur.

Notre démarche de numérique à impact répond à cette ambition. Elle vise à proposer des solutions cloud plus sobres, plus éthiques et plus maîtrisables, en phase avec les valeurs que nous partageons avec nos clients : responsabilité, ancrage local, exigence de résultat.

Le cloud de confiance, c'est une exigence concrète, conçue pour garantir l'ancrage français des données, la conformité réglementaire, la cybersécurité de haut niveau et une relation durable avec nos clients.

Ce livre blanc a été conçu comme un outil de dialogue et de lucidité au service des départements IT. Il vous aidera à :

- Comprendre les enjeux actuels de souveraineté numérique
- Identifier les bonnes pratiques pour limiter les risques dans le cloud,
- Clarifier le rôle stratégique que peut jouer un cloud souverain ou de confiance dans une stratégie numérique alignée sur vos valeurs.

Chez Sigma, nous croyons que souveraineté, performance et responsabilité ne sont pas des options incompatibles, mais des piliers d'un numérique digne de confiance — au service des utilisateurs, des organisations et de l'intérêt général.

1. CLOUD SOUVERAIN, CLOUD DE CONFIANCE : DES BASES POUR MAÎTRISER LES RISQUES

À mesure que les entreprises externalisent leurs systèmes d'information, la question de la confiance dans l'infrastructure cloud devient centrale. Il ne s'agit plus seulement de performance ou de coût, mais de maîtrise, de conformité et de sécurité juridique. C'est dans ce contexte que les notions de cloud souverain et de cloud de confiance prennent tout leur sens.

Cloud souverain : ancrer les données dans un cadre national

Le cloud souverain repose sur un principe simple mais fondamental : les données sont hébergées, traitées et administrées sur le territoire national, par des acteurs soumis uniquement au droit français ou européen.

Ce choix garantit :

- Une **localisation maîtrisée** des données
- Une **protection juridique renforcée**
- Une **conformité stricte** aux réglementations locales (RGPD, HDS, directives sectorielles)

Pour les entreprises manipulant des données sensibles (santé, défense, finance, collectivités), cette garantie est **indispensable**.

Cloud de confiance : viser un engagement au-delà de la localisation

Le cloud de confiance élargit la notion de souveraineté. Il ne se limite pas à la localisation des données, mais vise à empêcher toute forme d'intrusion non souhaitée, notamment par des puissances étrangères.

Il s'appuie sur :

- Des **certifications de sécurité** (SecNumCloud, ISO 27001…)
- Des **architectures techniques cloisonnées**
- Des **engagements contractuels forts** (clauses de non-transfert, audits, réversibilité)

Cette approche est particulièrement pertinente dans un contexte où certaines lois extraterritoriales (comme le Cloud Act ou la loi FISA) permettent à des États tiers d'accéder à des données hébergées hors de leur territoire.

Une réponse concrète aux enjeux de confiance et de responsabilité

Qu'il soit souverain ou de confiance, le cloud permet de :

- **Renforcer la confiance** : en garantissant que les données sensibles sont protégées contre les risques juridiques, techniques et géopolitiques.
- **Partager clairement les responsabilités** : en cas d'incident (cyberattaque, perte de données, non-conformité), le client peut se retourner contre un fournisseur soumis au droit français, avec des leviers de recours concrets.

À l'inverse, en cas d'hébergement dans un cloud non souverain, les recours sont souvent complexes, transfrontaliers et juridiquement incertains.

2. DE L'AUDIT AU CHOIX STRATÉGIQUE : MAÎTRISER L'AMONT D'UN PROJET CLOUD SOUVERAIN

La réussite d'un projet cloud de confiance ne repose pas uniquement sur le choix d'un fournisseur ou d'une technologie. Elle commence bien plus tôt, par une **analyse rigoureuse des données, des usages et des contraintes.**

Trop souvent sous-estimée, cette phase en amont conditionne la capacité de l'organisation à maîtriser les risques sur le long terme

Identifier ce qui doit être protégé

Quand on leur demande les priorités sur un cloud de confiance, les décideurs citent aujourd'hui la protection et la sécurité des données comme 1er argument dans près de 80 % des cas[4].

Toutes les données ne présentent pas le même niveau de sensibilité. Raison pour laquelle l'entreprise doit hiérarchiser ses actifs numériques :

- Les **données critiques** (financières, industrielles, RH, santé) doivent bénéficier d'un hébergement sécurisé, souvent sur des infrastructures souveraines ou certifiées.
- Les **données moins sensibles** (contenus marketing, données publiques, logs techniques) peuvent être hébergées dans des environnements plus ouverts, à condition de respecter les règles de base du RGPD.

Cette cartographie des données doit être croisée avec celle des applications et services : certains exigent une disponibilité continue (ex. : outils de production), d'autres une confidentialité absolue (ex. : dossiers médicaux, données de R&D).

Intégrer les contraintes réglementaires dès la conception

Le cadre réglementaire impose des obligations spécifiques selon la nature des données et le secteur d'activité :

- **RGPD** pour les données personnelles
- **HDS** pour les données de santé
- **DORA** pour les services financiers
- **NIS2** pour les entités essentielles et critiques
- **Obligations sectorielles** (éducation, défense, collectivités…)

Si vous négligez ces contraintes, vous vous exposez à des sanctions, mais aussi à de potentiels blocages opérationnels au moment d'un audit ou d'un changement de prestataire, par exemple.

Au moment de dresser votre cahier des charges cloud, vous devez connaître les réglementations qui s'appliquent pour vous et prévoir tous les impacts concrets sur votre infrastructure informatique.

[4] Etude Markess Exaegis "Cloud de confiance : où en est-on en 2025 En France ?"

Clarifier les responsabilités en cas d'incident

Un point souvent négligé dans les projets cloud est la **répartition des responsabilités**. En cas de perte de données, d'intrusion ou d'exploitation abusive, qui est responsable ? Le client ? Le fournisseur ? Les deux ?

Un contrat bien rédigé, adossé à un fournisseur souverain ou de confiance, permet de :

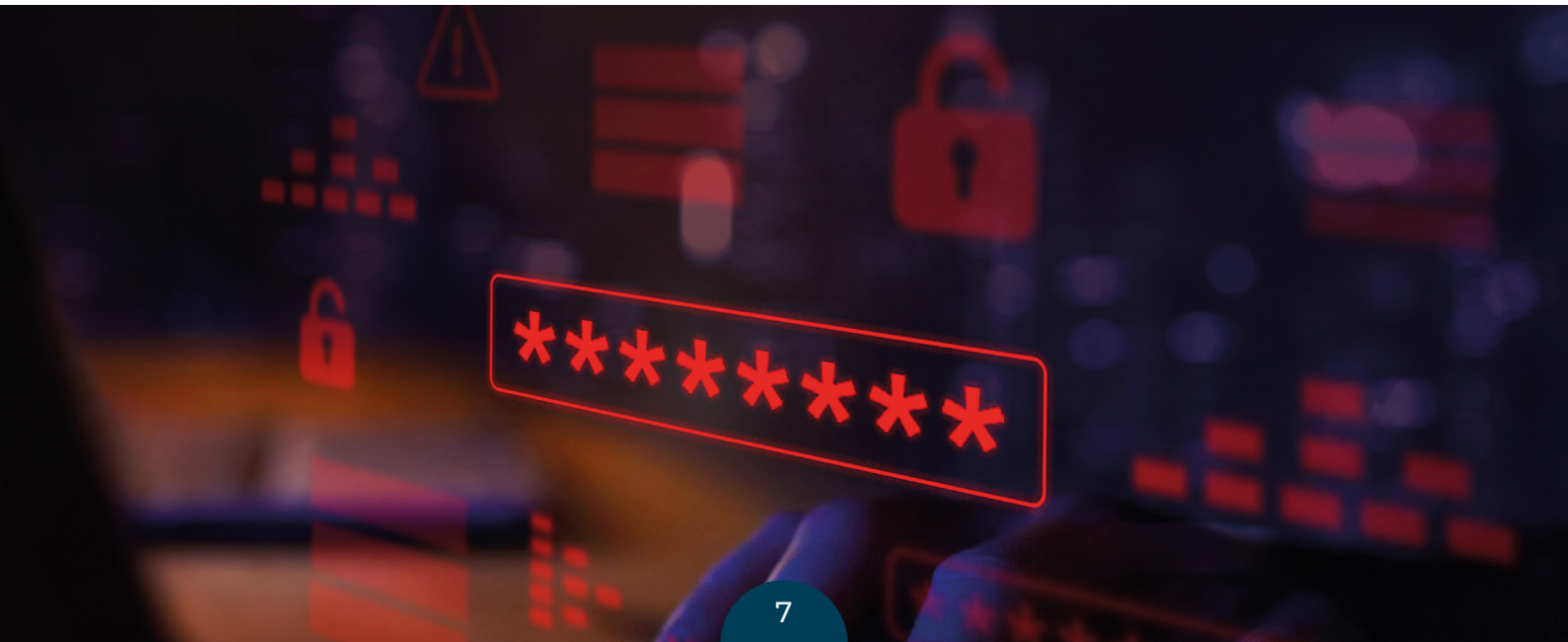
- Définir des **clauses de responsabilité claires** ;
- Prévoir des **mécanismes de recours** en cas de litige ;
- Garantir une **traçabilité optimale des accès et des traitements**.

Le cloud souverain comme levier de continuité et de sécurité

Migrer vers le cloud permet de répondre à des enjeux techniques et opérationnels majeurs :

- **Volumétrie** : capacité à absorber des charges importantes ;
- **Réactivité** : délais de traitement et de restauration
- **Interopérabilité** : compatibilité avec les systèmes existants ;
- **Réversibilité** : possibilité de changer de fournisseur facilement et sans perte de données.

Au-delà de ces enjeux techniques, privilégier un cloud qui soit souverain intègre une garantie de recours : en cas d'incident, le client peut se tourner vers un fournisseur soumis au droit français, avec des obligations de transparence et de coopération. Ce recours est beaucoup plus complexe si les données sont hébergées à l'étranger, notamment chez des acteurs soumis à des lois extraterritoriales.



3. ADAPTER LA STRATÉGIE CLOUD AUX USAGES MÉTIERS : ENTRE OPPORTUNITÉ ET VIGILANCE

La migration vers le cloud ne peut être envisagée de manière uniforme. Elle doit impérativement s'inscrire dans une stratégie adaptée aux objectifs métiers, aux contraintes techniques et aux capacités internes de chaque organisation. Cette adaptation permet de maximiser les bénéfices tout en identifiant et maîtrisant les risques inhérents à chaque contexte.

Extension de capacité : le cloud comme prolongement du SI

Dans un premier scénario, le cloud joue le rôle d'extension naturelle du système d'information. Il permet d'absorber des pics de charge temporaire, d'héberger des environnements de test ou encore d'externaliser certaines briques non critiques. Cette utilisation s'inscrit principalement dans un modèle IaaS (Infrastructure as a Service).

La priorité dans ce cadre est la maîtrise technique autour des performances, de la disponibilité et de la sécurité réseau. Cependant, ce modèle transfère une part significative du risque, antérieurement géré en interne, vers le fournisseur cloud, ce qui introduit un enjeu contractuel fort. En cas d'attaque ou d'incident, la responsabilité devient partagée entre client et prestataire, rendant essentiels des contrats clairs et des mécanismes de gouvernance solides.

Modernisation : accélérer les développements

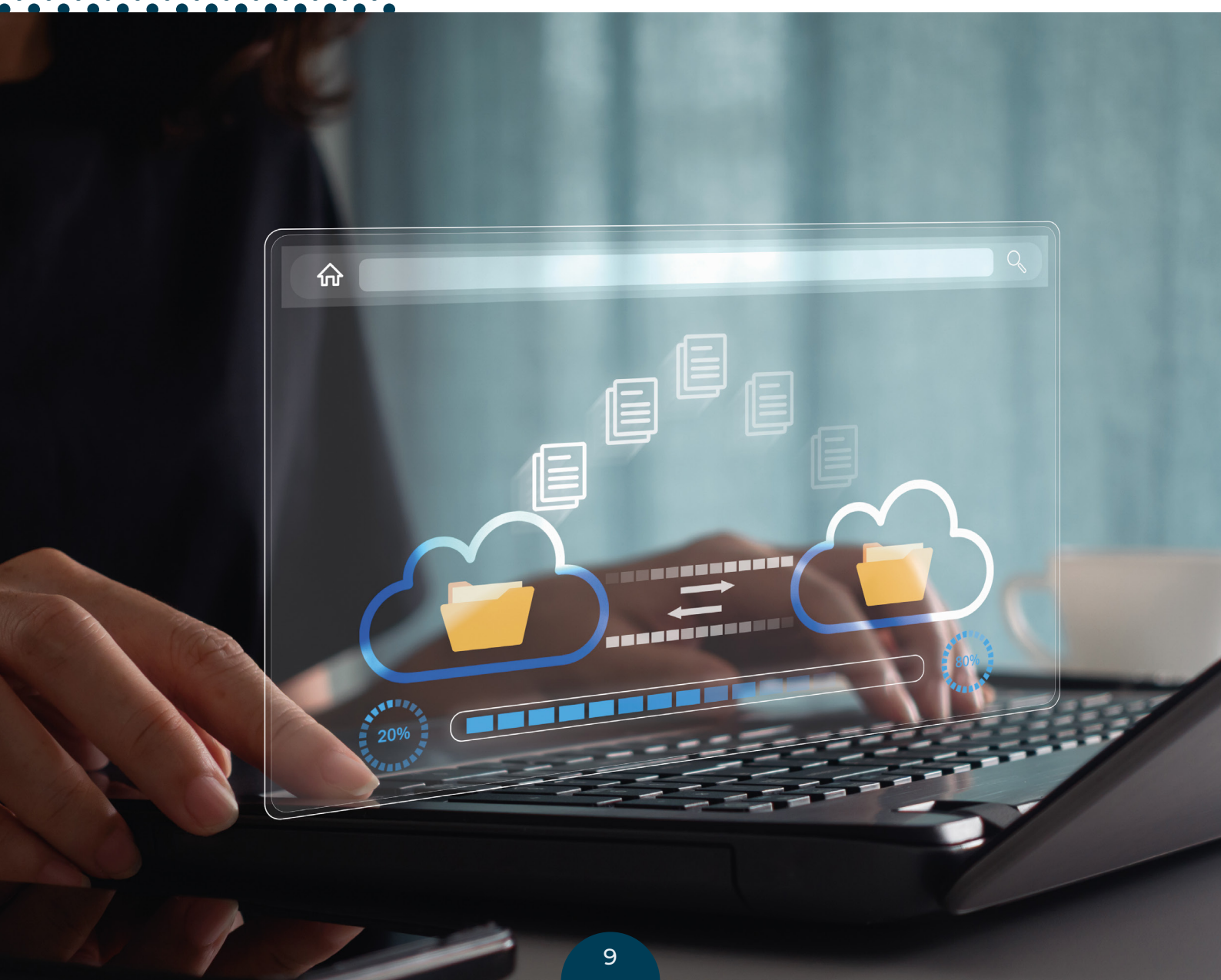
Le cloud devient ensuite un puissant levier d'innovation via des plateformes PaaS (Platform as a Service) capables de réduire le time-to-market grâce à des outils de développement accélérés et l'intégration de services avancés (intelligence artificielle, IoT, big data, etc.).

La priorité s'oriente ici vers la richesse fonctionnelle et la flexibilité organisationnelle. Ce contexte expose toutefois à un risque organisationnel notable : le manque de compétences internes pour gérer ces environnements complexes peut engendrer des difficultés d'interopérabilité, de sécurité, et surtout de réversibilité. Une dépendance excessive envers certains fournisseurs ou consultants peut rendre le changement d'environnement coûteux, voire même compromettre la continuité des services.

Transformation globale :
pour une souveraineté étendue

Au-delà des infrastructures, la transformation globale couvre désormais l'intégration complète des outils bureautiques et collaboratifs dans le cloud souverain.

L'objectif est d'atteindre une souveraineté non seulement technique mais aussi opérationnelle et fonctionnelle sur l'ensemble des usages quotidiens. Cette approche permet de maîtriser l'ensemble du périmètre IT, limitant ainsi les risques liés à la fuite ou à la perte de contrôle sur des données critiques, tout en favorisant l'agilité métier.



4. METTRE EN PLACE DES PRATIQUES CONCRÈTES POUR LIMITER LES RISQUES

Pour réussir une migration vers le cloud souverain tout en maîtrisant les risques, il est essentiel d'adopter des pratiques opérationnelles tangibles et rigoureuses. Ces bonnes pratiques couvrent plusieurs dimensions : la sécurité des données, la qualité des partenaires, ainsi que la formation et l'équipement des équipes internes.

Sécuriser les données dès la conception du projet

La sécurité des données ne doit jamais être une réflexion a posteriori. Elle nécessite d'être intégrée dès la phase de conception avec notamment la mise en oeuvre du principe de sécurité dès la conception (**security by design**). Cela implique :

- L'identification systématique des données sensibles et critiques,
- La mise en place de mécanismes robustes de chiffrement, idéalement gérés côté client pour préserver la souveraineté des clés,
- Le contrôle d'accès strict et granulaire aux ressources cloud,
- La surveillance continue des environnements et la détection proactive des incidents.

Ces mesures, tout en garantissant la confidentialité et l'intégrité des données, favorisent également la conformité réglementaire avec les exigences de la RGPD et autres normes sectorielles.

S'appuyer sur des partenaires qualifiés

Le choix des partenaires est un facteur clé de succès. Il ne suffit pas de sélectionner un fournisseur sur la seule base d'un label « cloud souverain ». Il est impératif d'évaluer la capacité réelle du prestataire à :

- Offrir une infrastructure et des services conformes aux normes de sécurité et de souveraineté,
- Fournir des garanties contractuelles claires sur la gestion des données (localisation, accès, confidentialité),
- Assurer une interopérabilité et une réversibilité avec les systèmes existants,
- Apporter un support technique réactif et expert ainsi qu'un accompagnement à la migration.

Les entreprises doivent privilégier des fournisseurs locaux ou européens de confiance pour réduire les risques liés à la dépendance technologique et aux enjeux géopolitiques.

Il est important de choisir le bon type de cloud (public, privé, hybride) en fonction de la criticité des données. Par exemple, un cloud public peut convenir pour des environnements de test, mais un cloud privé souverain est préférable pour des données RH ou financières.

CRITICITÉ	CONFIDENTIALITÉ	TYPE D'HÉBERGEMENT (EXEMPLES)
1 VITAL	1. Secret (Une divulgation peut compromettre l'avenir de l'entreprise)	Cloud souverain fortement recommandé ou On-Premise. Risque élevé sur les hyperscalers étrangers.
2 IMPACT BUSINESS FORT	2. Confidentiel (Une divulgation peut avoir un impact négatif sur l'image de l'entreprise)	Cloud souverain préférable. Usage possible de Cloud public avec restrictions. On-Premise selon réglementation.
3 IMPACT FAIBLE	3. Public (L'information peut être transmise)	Cloud public type AWS, Cloud souverain ou On-Premise, selon coûts et besoins.

INFOGRAPHIE : TABLEAU DE CLASSIFICATION POUR LE CHOIX DE L'HÉBERGEMENT

A. LIMITES ET DÉFIS DU CLOUD SOUVERAIN FRANÇAIS : PUISSANCE ET INNOVATION

Il est important de reconnaître que, malgré des avancées notables, le cloud souverain français rencontre encore des contraintes significatives en matière de capacités de calcul et d'innovation, notamment pour les entreprises ayant des besoins très élevés ou spécifiques. Aujourd'hui, seuls les hyperscalers internationaux disposent de l'échelle et des technologies (notamment en intelligence artificielle, big data, calcul haute performance) capables de répondre efficacement à ces exigences.

Cette réalité impose aux décideurs une évaluation pragmatique des usages et des besoins, avec la conscience que le cloud souverain, en tant que gage de souveraineté et de conformité, ne couvre pas toujours toutes les exigences opérationnelles innovantes.

B. LE MULTI-CLOUD, UNE SOLUTION D'ÉQUILIBRE

Face à cette contrainte, la stratégie de multi-cloud apparaît comme une solution équilibrée. Elle consiste à combiner l'usage du cloud souverain — pour les données les plus sensibles et les charges critiques — avec les capacités offertes par des hyperscalers performants pour les workloads intensifs, les développements innovants et les besoins de scalabilité.

Le multi-cloud permet ainsi d'optimiser à la fois la maîtrise des risques liés à la souveraineté et la performance technique nécessaire au développement des applications métiers à fort enjeu d'innovation. Cette approche nécessite cependant une gouvernance rigoureuse, une interopérabilité maîtrisée et un pilotage expert des contrats et des flux de données.

Former et outiller les équipes

La montée en compétence des équipes internes est un enjeu souvent sous-estimé, mais fondamental. Le cloud souverain introduit des environnements technologiques spécifiques et parfois complexes à maîtriser. Pour réduire les risques humains et organisationnels il est recommandé de :

- Former les DSI, responsables sécurité et équipes opérationnelles sur les spécificités du cloud souverain et ses bonnes pratiques,
- Mettre à disposition des outils adaptés pour automatiser la gestion des accès, le monitoring et la sécurité,
- Promouvoir une culture de vigilance permanente autour des questions de sécurité et de conformité, et mettre en place une veille sur les risques associés à ses fournisseurs clés.

Une équipe bien outillée et formée est une première ligne de défense efficace pour limiter les risques liés à la gestion des environnements cloud souverains.

S'appuyer sur des partenaires qualifiés

Le choix du prestataire est un **acte stratégique.** Il doit être aligné avec le niveau d'exigence de l'organisation.

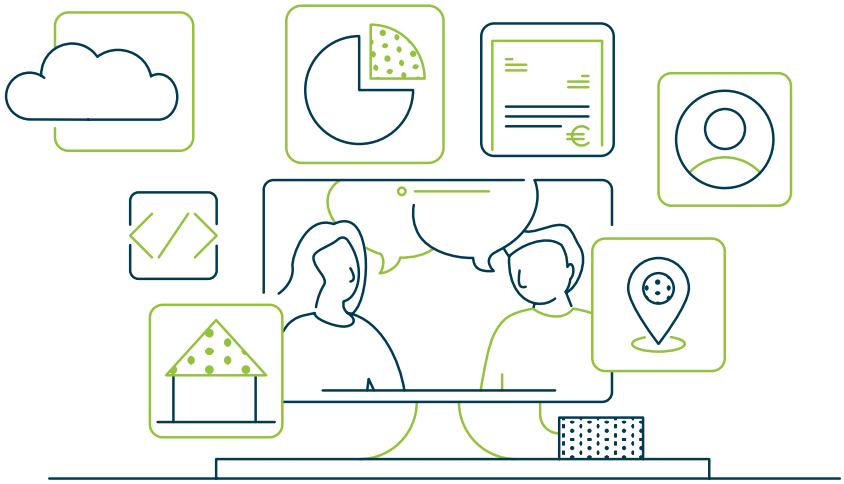
- **Vérifier les certifications** (ISO 27001, HDS…) et les engagements contractuels du fournisseur.
- Pour les données sensibles, **privilégier des prestataires français ou européens**, non soumis à des réglementations extraterritoriales comme le Cloud Act américain, qui autorise l'accès aux données par les autorités, même si elles sont hébergées hors des États-Unis.

5. ADOPTER UNE POSTURE DE PRUDENCE DANS UN CONTEXTE EN MUTATION

Une offre souveraine encore en construction

Si la souveraineté numérique est devenue un enjeu européen majeur, l'offre de cloud souverain reste incomplète et fragmentée à l'heure actuelle :

- Le référentiel SecNumCloud, porté par l'ANSSI, reste à ce jour spécifique à la France.
- Le projet de certification EUCS (European Cybersecurity Certification Scheme for Cloud Services) est toujours en discussion. En 2025, le niveau de sécurité le plus élevé, dit « High+ », a été retiré faute de consensus entre les États membres.
- Cette absence d'harmonisation à l'échelle de l'UE freine l'émergence de véritables champions européens du cloud, capables de rivaliser avec les hyperscalers américains ou chinois.



Calquer sa stratégie sur les cas d'usage

Il n'existe pas de solution cloud unique à privilégier pour tous. La stratégie cloud doit être adaptée aux cas d'usage :

- Au sein d'un service RH externalisé, par exemple, le recours à un cloud européen conforme RGPD s'impose.
- Pour une infrastructure avec des données financières ou industrielles, par exemple, on va privilégier un cloud souverain avec des clauses de réversibilité, de chiffrement et des responsabilités juridiques clairement établies.

En cas de cyberattaque ou de fuite de données, le partage de responsabilité entre le client et le fournisseur devient un levier essentiel. En effet, le recours devant un tribunal national est toujours possible en cas de souci… Mais beaucoup plus compliqué avec un acteur soumis à une juridiction étrangère.

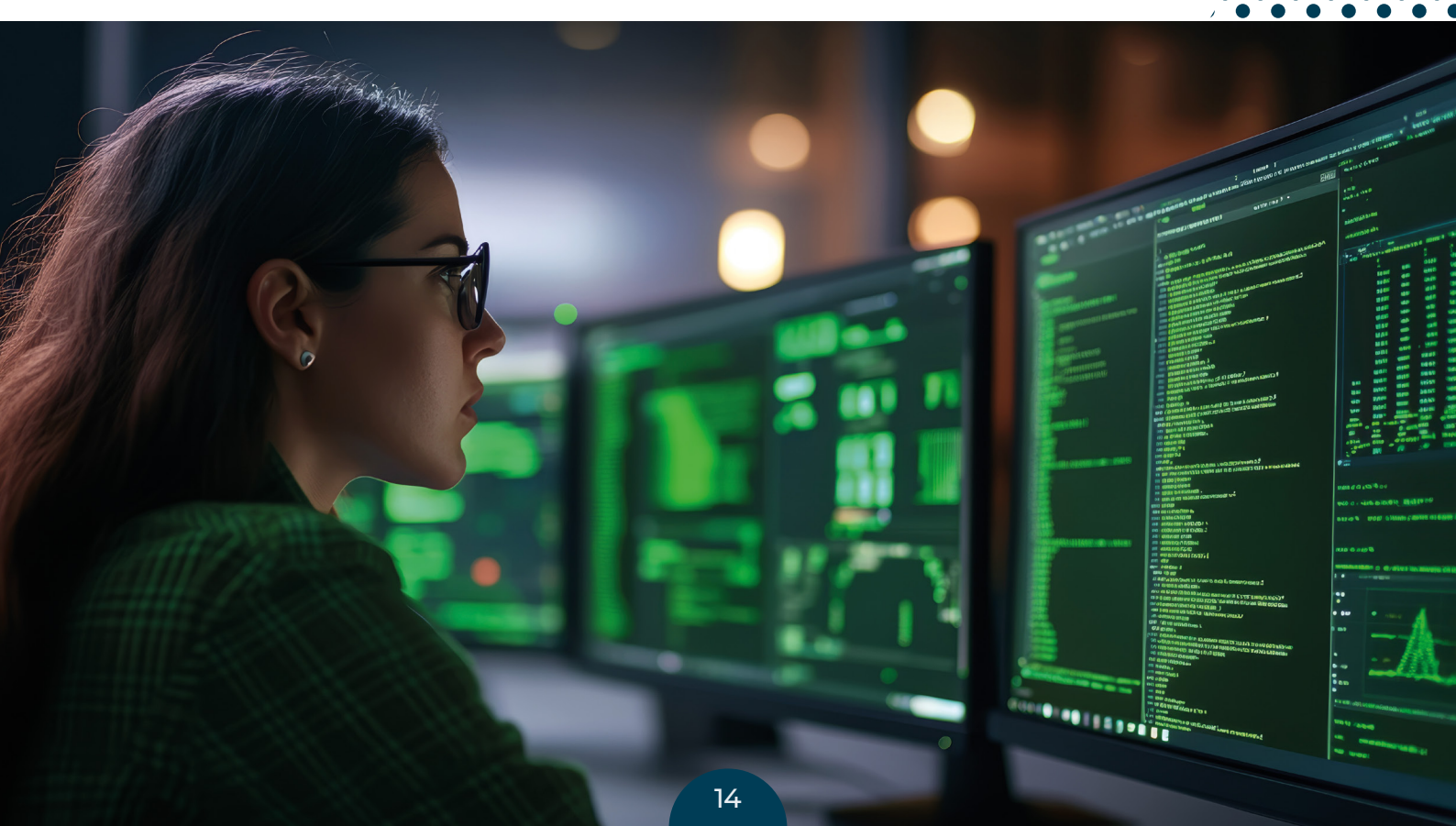
CONCLUSION

Dans un contexte marqué par l'accélération des enjeux géopolitiques, réglementaires et technologiques, il est clair que le cloud souverain constitue un pilier stratégique indispensable pour garantir la maîtrise, la sécurité et la conformité du système d'information français. Cependant, sa capacité à couvrir l'ensemble des besoins en puissance de calcul, notamment pour l'innovation poussée, reste encore limitée par rapport aux hyperscalers mondiaux.

Se pose alors une question fondamentale : comment allier souveraineté et performance ? La réponse réside dans une stratégie cloud hybride ou multi-cloud, adaptée à chaque usage métier, intégrant des solutions souveraines pour les données sensibles, associées à des capacités avancées proposées par des acteurs internationaux reconnus.

Ainsi, la souveraineté numérique ne doit pas se faire au prix de l'isolement ou de la stagnation technologique, mais par un équilibre stratégique. La maîtrise des risques, la conformité réglementaire renforcée et la capacité à innover doivent devenir des vecteurs complémentaires, permettant aux acteurs publics et privés de construire un écosystème numérique durable, responsable et compétitif.

Le gouvernement européen, en poursuivant ses efforts pour harmoniser le cadre réglementaire et encourager le développement d'un cloud européen puissant, jouera un rôle clé dans cette transformation. En attendant, les entreprises françaises doivent s'appuyer sur une approche pragmatique, volontaire, et résolument orientée vers la cohérence stratégique entre souveraineté, performance et innovation.



À PROPOS DE SIGMA

Sécurisez vos données et optimisez votre activité

Sigma Informatique, acteur majeur de l'infogérance et de l'hébergement IT en France, garantit la **sécurité de vos données** dans nos *Datacenters* haute disponibilité en France. Nos **solutions à la carte** vous permettent de bénéficier de **hauts niveaux de services** grâce à un interlocuteur dédié, un support en présentiel disponible 24/7/365 et des équipes d'architectes et d'experts certifiés.

Cloud Services

Gardez l'autonomie dans la gestion de votre infrastructure

- Espaces d'hébergement
- Cloud IaaS SIGMA
- Cloud PaaS
- Services Réseau et Sécurité
- Plateforme Kubernetes & DevOps

Services Managés

Profitez de prestations modulaires en fonction de vos besoins

- Infogérance Full Stack
- Clouds Managés Azure / AWS / GCP
- Performance & Sécurité Managée
- Supervision et Administration 24/7/365
- Gestion Microsoft 365
- Accompagnement
- Observabilité

Cybersécurité

Construisons ensemble votre résilience cyber

- Sensibilisation Cyber des collaborateurs
- Renforcement de la surveillance de votre SI avec un SIEM et SOC as a service
- Stratégie Zero Trust
- Parcours de sensibilisation
- Conformité NIS2, DORA, ISO27001
- Numérique Responsable

Les + externalisation du SI

Datacenters tiers III interconnectés en France

5 salles IT, 500 baies, 5000 serveurs supervisés

Accès, supervision, administration, *service desk*

SIGMA NUMÉRIQUE À IMPACT ETIX EVERYWHERE

À PROPOS DE SIGMA

Sigma est une entreprise du numérique, spécialisée dans l'édition et l'intégration de logiciels et de solutions sur mesure, l'externalisation de systèmes d'information et les solutions cloud, la cybersécurité et la valorisation des données.

Notre raison d'être :
« Apporter à notre écosystème des solutions numériques qui contribuent à un futur désirable dans lequel chacun et chacune trouve sa place ».

Nous servons votre performance économique, sociale et environnementale en révélant les potentiels de vos écosystèmes informatiques.

Nous militons pour un numérique à impact permettant de construire, avec vous, des services numériques utiles aux femmes et aux hommes, dans le respect du vivant.

Notre trajectoire : innover pour vous apporter des solutions éco-conçues.
D'ici 2026 : -40% de nos émissions GES et +50 % de nos solutions éco-conçues.

SiGMA
NUMÉRIQUE À IMPACT

La Gesvrine - 8 rue Newton
La Chapelle-sur-Erdre
Tel. : +33 (0)2 40 37 14 00
https://www.sigma.fr
@groupesigma

Nantes
Paris
Lyon
Toulouse
Strasbourg

700 collaborateurs sur 5 implantations nationales

10 partenaires technologiques majeurs

2200 clients

75 M€ de CA

5 piliers numériques majeurs

- Édition et intégration
- Solutions sur-mesure
- Data valorisation
- Infogérance et Cloud services
- Cybersécurité