CGI BUSINESS CONSULTING

SE PRÉPARER À L'APRÈS-QUANTIQUE : UNE TRANSITION DÉCISIVE POUR LA SÉCURITÉ NUMÉRIQUE

Construire aujourd'hui les fondations d'une cybersécurité prête pour l'ère quantique.

INTRODUCTION

L'informatique quantique quitte progressivement les laboratoires pour entrer dans l'ère industrielle. Ses promesses sont immenses : optimiser des chaînes logistiques complexes, accélérer la recherche médicale, concevoir de nouveaux matériaux ou encore transformer la puissance analytique des entreprises.

Mais cette avancée majeure s'accompagne d'un défi tout aussi considérable : la remise en question profonde des mécanismes de cybersécurité qui protègent aujourd'hui nos données et nos infrastructures.

À l'horizon des prochaines années, l'essor de l'informatique quantique — appelée à compléter et renforcer l'informatique classique plutôt qu'à la remplacer — fera franchir un cap décisif aux capacités de calcul. Cette évolution rendra vulnérables de nombreux protocoles cryptographiques actuels. Certains acteurs l'ont d'ores et déjà anticipée en collectant des données chiffrées, dans l'attente de pouvoir les déchiffrer ultérieurement, faisant peser une menace durable sur la confidentialité, dès à présent, et par la suite sur l'intégrité des données et la confiance numérique.

Face à cette rupture annoncée, des questions essentielles s'imposent : ***comment préparer les organisations pour qu'elles ne subissent pas le choc, mais l'anticipent avec maîtrise et lucidité ? Quelles données doivent être protégées dès aujourd'hui ? Comment adapter les stratégies de cybersécurité pour rester résilient dans un monde post-quantique ?***

Notre démarche d'accompagnement répond précisément à ces enjeux. Elle vise à guider les organisations dans leur transition vers une cybersécurité post-quantique, en alliant vision stratégique, maîtrise technologique et feuille de route opérationnelle.

SOMMAIRE

01

POURQUOI ANTICIPER L'ÈRE QUANTIQUE DÈS AUJOURD'HUI ?

L'informatique quantique n'est plus un concept lointain. Avec l'accélération des investissements et des avancées technologiques, elle s'apprête à transformer profondément nos usages numériques — et en particulier, nos fondations cryptographiques.

Les signaux clés

- **Progression fulgurante** des capacités quantiques : de 53 qubits en 2019 à plus de 6 000 en 2024.
- **Prévision de maturité cryptographique** estimé entre **2030 et 2035**.
- **Enjeu géopolitique et économique majeur** pour les États comme pour les entreprises.
- **Risque émergent : "Harvest Now, Decrypt Later" ou "récolter maintenant, déchiffrer plus tard"**: des acteurs malveillants stockent aujourd'hui des données chiffrées, en attendant de pouvoir les déchiffrer demain.

Pourquoi agir maintenant ?

Parce que les données les plus sensibles — santé, secrets industriels, contrats, archives stratégiques — conservent leur caractère critique dans la durée, y compris dans dix ans.

Ne pas se préparer expose à un risque majeur : **la rupture de confiance numérique**.

02

MENACE QUANTIQUE : COMPRENDRE LES RISQUES ET LES DONNÉES À PROTÉGER

Comment fonctionne un ordinateur quantique ?

Contrairement aux processeurs classiques, les ordinateurs quantiques utilisent des **qubits**, capables de calculer simultanément toutes les valeurs possibles grâce aux principes spécifiques à la physique quantique que sont :

- **la superposition des états,**
- **l'intrication des particules,**
- **et l'approche probaliste d'un résultat.**

Résultat : certains algorithmes dit « quantiques », comme **Shor** ou **Grover**, pourraient réduire drastiquement le temps nécessaire pour casser les cryptographies actuelles.

Quels impacts sur la cybersécurité ?

Deux risques majeurs émergent :

- **Usurpation d'identité numérique** : se faire passer pour un utilisateur, une organisation ou un système de confiance afin de procéder à des signatures frauduleuses, détourner des certificats ou prendre le contrôle de systèmes critiques.
- **Perte de confidentialité massive** : accès à des archives stratégiques, secrets industriels, données de santé.

De ces risques numériques dérivent une grande quantité de risques majeurs de toutes natures, pouvant impacter toutes les organisations.

Quelles données doivent être protégées dès aujourd'hui ?

Données prioritaires

- Secrets de défense et d'intérêt national
- Secrets industriels et avantages compétitifs
- Données personnelles sensibles à longue durée de vie (santé, finances…)
- Contrats, archives classifiées, transactions critiques

Quelles actions les organisations peuvent-elles réaliser pour s'organiser ?

Démarche de protection

- Identifier les données sensibles à horizon long
- Cartographier les flux et dépendances technologiques
- Évaluer les zones d'exposition et leur niveau de maturité/agilité face aux changements qui s'annoncent
- Prioriser les plans de migration cryptographique

03

CADRES ET STANDARDS : UNE TRANSITION DÉJÀ ENGAGÉE

Standards internationaux

La transition vers la cryptographie post-quantique est désormais cadrée par des standards reconnus.

Le **NIST (États-Unis)** a formalisé les premiers algorithmes post-quantiques à travers :

- **FIPS 203** : CRYSTALS-Kyber (chiffrement / échange de clés),
- **FIPS 204 :** CRYSTALS-Dilithium (signature),
- **FIPS 205** : SPHINCS+ (signature),
- **FIPS 206** (en cours) : FALCON,
- **HQC** (en cours de sélection).

En Europe, la directive **NIS2 (2022)** impose une sécurité cryptographique « à l'état de l'art », entendue comme la capacité à **faire évoluer rapidement les algorithmes cryptographiques** — un principe clé de crypto-agilité.

Par ailleurs, la Commission européenne et le **NIS Cooperation Group** encouragent les États membres à définir des **feuilles de route nationales** pour la transition vers la cryptographie post-quantique, avec des jalons indicatifs : démarrer la transition avant **fin 2026** et viser une adoption pour les **infrastructures critiques d'ici 2030**.

Position et recommandations de l'ANSSI

Dans une logique de convergence des standards, l'**ANSSI** s'inscrit dans l'alignement des standards du NIST et recommande aux organisations, publiques comme privées, de :

- Intégrer la **menace quantique** dans leurs analyses de risques cryptographiques,
- Réaliser **un inventaire des usages cryptographiques** existants,
- **Planifier la transition** vers des solutions intégrant la cryptographie post-quantique selon les standards NIST.

L'ANSSI préconise également l'usage de **mécanismes hybrides** (combinaison d'algorithmes classiques éprouvés et post-quantiques) comme mesure intermédiaire, afin de maintenir le niveau de sécurité actuel tout en renforçant la résistance face à la menace quantique.

Plusieurs guides et référentiels sont en cours de mise à jour pour intégrer ces enjeux, notamment :

- le **guide des mécanismes cryptographiques** (ex-annexe B1 du RGS),
- le r**éférentiel IPsecDR**.

À ce stade, les recommandations relatives à la cryptographie post-quantique ne sont pas encore obligatoires. Les exigences réglementaires en matière de cryptographie concernent aujourd'hui des périmètres spécifiques (données classifiées de défense, certains systèmes d'information vitale, certifications et qualifications de produits).

Toutefois, ces cadres réglementaires et techniques évoluent et devraient intégrer progressivement la cryptographie post-quantique à partir de 2027 pour certaines catégories de produits qualifiés.

État du marché : expérimentations et adoption

L'écosystème fournisseurs se structure déjà :

- **Constructeurs HSM** (coffre-fort des secrets) : intégration des nouveaux algorithmes de cryptographie post-quantique (PQC).
- **Éditeurs PKI** (générateur des certificats cryptograhiques organisés en chaine de confiance) : premières versions compatibles PQC.
- **Solutions de confiance numérique** (utilisateur de certificats cryptographiques pour proposer un service de confiance): tests d'impact et prototypes opérationnels.

Les secteurs les plus sensibles — défense, banque, santé, énergie, télécoms — sont déjà engagés ainsi que les entités régulées à enjeux systémiques engagées à se mettre en conformité NIS2.

04

COMMENT SE PRÉPARER ? LES LEVIERS POUR LES ORGANISATIONS

Premiers pas recommandés

- Réaliser une analyse de **maturité post-quantique pour évaluer le niveau d'exposition et de risques**
- Qualifier les systèmes et les organisations dépendants de principes cryptographiques et évaluer leur niveau de compatibilité et d'agilité face à la migration qui s'annonce
- Mettre en place un plan de **migration cryptographique**
- Anticiper les impacts opérationnels (performances, intégration, contrats) au travers de tests des bibliothèques de cryptographiques post-quantique dans des conditions représentatives des environnements cibles

05

L'ACCOMPAGNEMENT CGI BUSINESS CONSULTING POUR CONSTRUIRE UNE STRATÉGIE DE CRYPTOGRAPHIE POST-QUANTIQUE (PQC) ROBUSTE ET ACTIONNABLE

CGI Business Consulting accompagne les organisations dans la définition d'un plan stratégique PQC, fondé sur la priorisation des risques métiers liés à la future exploitation des failles cryptographiques et sur l'anticipation des contraintes liées au déploiement de certificats et mécanismes cryptographiques résistants au quantique.

1. ANALYSE DES RISQUES MÉTIERS

2. IDENTIFICATION DES FREINS À LA MIGRATION

3. ELABORATION D'UN PLAN STRATÉGIQUE

Une démarche complète, structurée et immédiatement actionnable pour anticiper la rupture cryptographique et **sécuriser durablement** vos actifs critiques.

1. ANALYSE DES RISQUES MÉTIERS : UNE DÉMARCHE TOP-DOWN

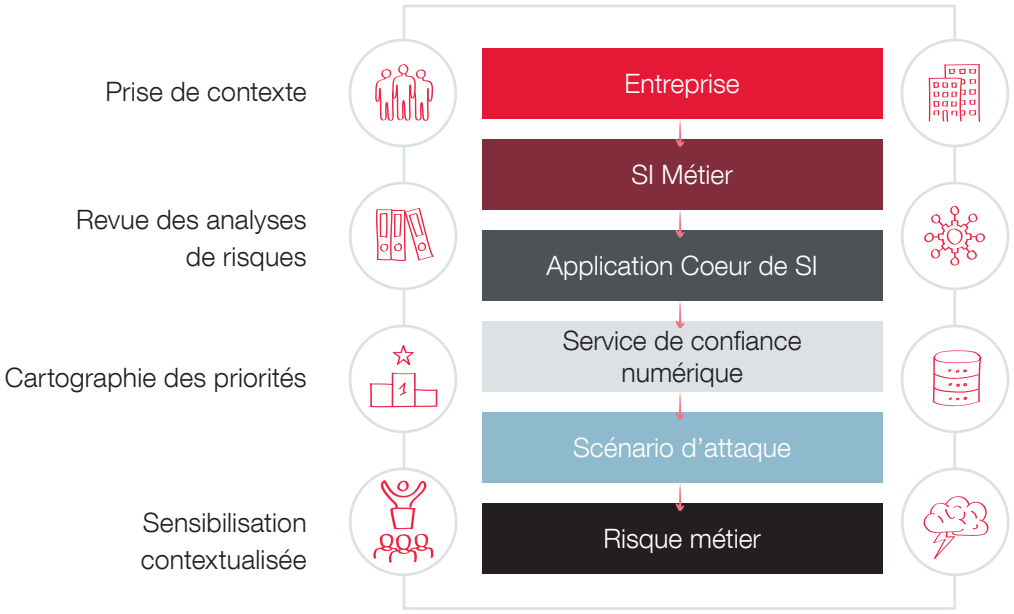
La transition vers la PQC ne peut se réduire à un simple remplacement technologique : elle doit d'abord répondre aux enjeux business.

Objectifs

- Identifier les processus métiers dépendants de services numériques de confiance basés sur des principes cryptographiques.
- Évaluer les conséquences d'une compromission future (vol, falsification, indisponibilité des données).
- Prioriser les risques selon leur impact, probabilité et criticité opérationnelle.

Résultats clés

- Une vision claire des actifs sensibles, des expositions majeures et des scénarios de menace pertinents.
- La capacité de répondre à une question stratégique (cf schéma)



2. IDENTIFICATION DES FREINS À LA MIGRATION : UNE DÉMARCHE BOTTOM-UP

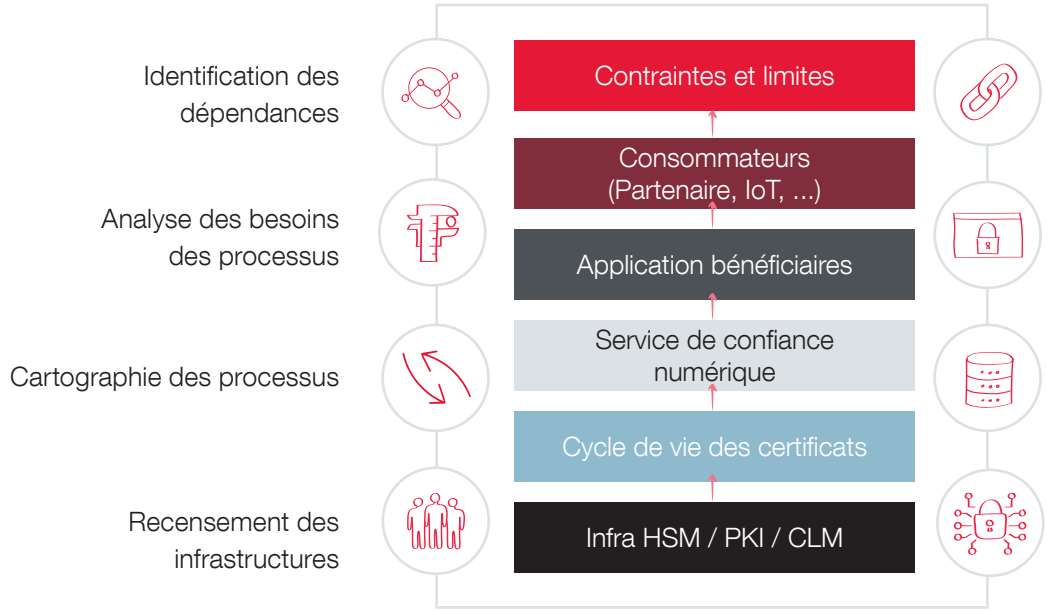
À partir de la réalité du terrain, nous menons une analyse détaillée des dépendances technologiques et techniques.

Objectifs

- Identifier les consommateurs de certificats numériques et utilisateurs de mécanismes cryptographiques (applications, partenaires, IoT, infrastructures) qui devront supporter les standards PQC.
- Identifier les contraintes techniques, réglementaires et organisationnelles qui peuvent ralentir la transition.
- Évaluer la maturité des chaînes de délivrance de certificats numériques (HSM / PKI / CLM) face aux standards PQC émergents et aux besoins d'adaptation.

Résultats clés

- Une compréhension complète du cycle de vie des certificats, des architectures de services associés et des leurs évolutivités vers les algorithmes PQC.
- Un panorama précis des verrous techniques (limite de stockage des futurs certificats, obsolescence technologique…) et organisationnels (dépendance à partenaires business contraignants, complexité métier…), des impacts sur l'existant (révision des capacités, montée de version, remplacement technologique…) et des coûts potentiels.



3. IMPACT PAR TYPE A ELABORATION D'UN PLAN STRATÉGIQUE

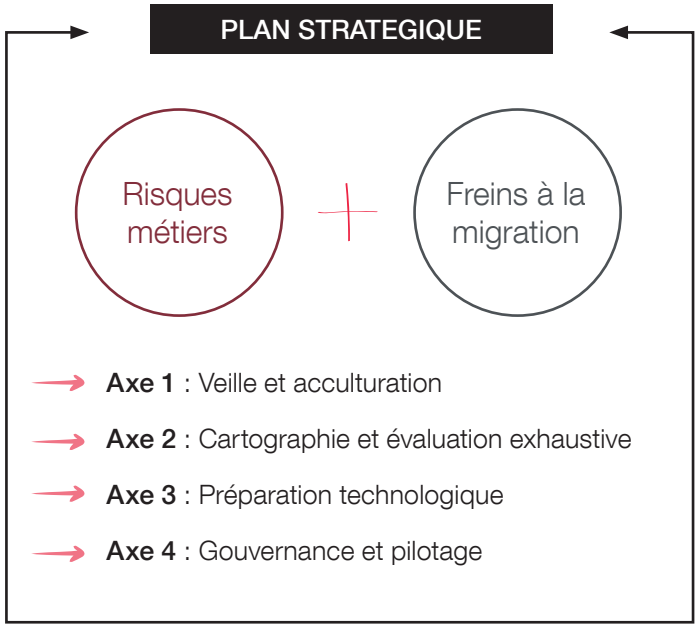
Fort de la convergence des analyses TOP-DOWN et BOTTOM-UP, CGI Business Consulting construit un plan d'action réaliste, progressif et pilotable.

Objectifs

- Définir une trajectoire de transformation priorisée et réalisable.
- Anticiper les évolutions technologiques, les changements de standards, et l'arrivée des mécanismes cryptographiques résistants au quantique.
- Intégrer les impacts sur l'écosystème interne et externe (applications métier, partenaires, équipements, objets connectés…).

Livrables

- Roadmap PQC, structurée en scénarios de migration.
- Plan d'investissement et estimations budgétaires.
- Modèle de gouvernance pour piloter la transformation cryptographique.
- Recommandations opérationnelles pour sécuriser durablement vos actifs critiques.



Notre approche permet aux organisations d'anticiper la rupture cryptographique, de réduire les risques associés à la compromission des mécanismes actuels et de préparer sereinement l'adoption des standards PQC.

L'ère post-quantique n'est pas une hypothèse : elle est déjà engagée.

Les organisations qui se préparent dès aujourd'hui protégeront demain :

- *leur souveraineté,*
- *leur compétitivité,*
- *et la confiance de leurs clients et usagers.*

CGI Business Consulting est engagé à vos côtés pour anticiper cette transition et construire un futur numérique résilient.

CONTACTS

- **LABOUREAU Pierre**

  Vice-Président en charge des offres de Cybersécurité

  pierre.laboureau@cgi.com

- **KULPA-BOGOSSIAN Raffi**

  Manager spécialiste en gestion des certificats numériques et sécurité des échanges en ligne

  raffi.kulpabogossian@cgi.com

CGI BUSINESS CONSULTING

Chez CGI Business Consulting, cabinet de conseil majeur en France, nous sommes audacieux par nature.
Grâce à son intimité sectorielle et à sa capacité à mobiliser des expertises diverses, CGI Business Consulting apporte aux entreprises et aux organisations des solutions de conseil audacieuses et sur mesure, pour une réussite stratégique et opérationnelle de leurs projets de transformation.
Nos 1 000 consultants accompagnent nos clients dans la conduite et la mise en œuvre de leurs projets de transformation, dans une relation franche et de confiance, pour leur permettre de prendre les bonnes décisions.
Fondée en 1976, CGI figure parmi les plus importantes entreprises de services-conseils en technologie de l'information (TI) et en management au monde. Elle aide ses clients à atteindre leurs objectifs, notamment à devenir des organisations numériques axées sur le client.

cgi.fr/conseil

L'audace par nature