FORUM DES COMPÉTENCES
Cyber & Résilience

QuRISK
Quantum Risk & Cybersecurity

Forum des compétences

Livre Blanc « Quantique & Cybersécurité »

Quantum Risk Advisory (QuRISK)
www.qurisk.fr

Sommaire

Résumé Exécutif du
Livre Blanc « Quantique & Cybersécurité »

Résumé Exécutif (1/2)

Les **technologies quantiques** exploitent les propriétés de la mécanique quantique pour les appliquer sur des technologies actuelles et donner **l'informatique quantique**, **la communication quantique** et **les capteurs quantiques**.

Les technologies quantiques

- **L'informatique quantique**
- **La communication quantique**
- **Les capteurs quantiques**

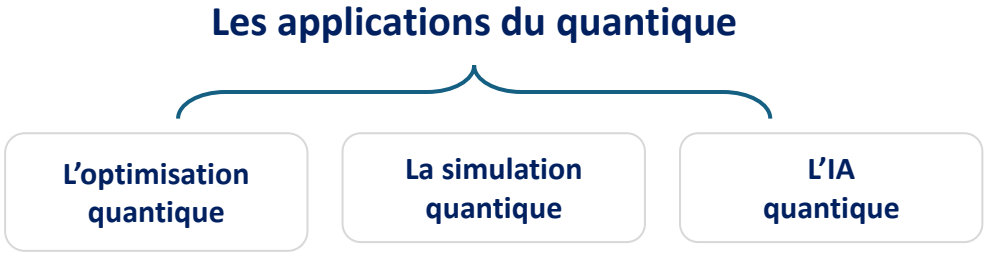
Pour le secteur financier, ces avancées représentent à la fois une menace critique et des opportunités véritablement disruptives. En matière de menaces, les risques liés à l'informatique quantique se structurent autour de deux volets complémentaires :

Pour remédier à la cybermenace quantique, les organisations sont désormais appelées à **migrer vers des protocoles cryptographiques post-quantiques (PQC)**, en s'appuyant sur un cadre méthodologique structuré comme celui-ci:

1. **Sensibilisation** à la cybermenace et à la migration PQC
2. **Evaluations** de la cybermenace et des protocoles vulnérables
3. **Expérimentation** de cas d'usages et de protocoles PQC
4. **Déploiement** massif des protocoles PQC

Résumé Exécutif (2/2)

Par ailleurs, les **applications de l'informatique quantique** se structurent autour de trois grandes familles : **l'optimisation**, **la simulation** et **l'intelligence artificielle quantique**. Elles offrent aux secteurs critiques, notamment la finance, une large gamme de cas d'usage, tels que l'optimisation avancée de portefeuilles, la détection proactive de fraude, la modélisation de risques complexes ou encore l'amélioration des algorithmes d'analyse prédictive.



Ce livre blanc propose une vision claire, opérationnelle et pragmatique des enjeux quantiques. Son objectif est d'aider le secteur financier à renforcer sa résilience, sa sécurité et sa souveraineté dans une décennie où le quantique deviendra un facteur déterminant de compétitivité, tout en permettant aux institutions financières de tirer parti des multiples opportunités offertes par ces technologies émergentes.

Introduction du
Livre Blanc « Quantique & Cybersécurité »

Introduction

Le secteur financier est à l'aube d'une transformation majeure portée par les technologies quantiques. Ces avancées redéfiniront les capacités d'analyse, d'optimisation et de modélisation des banques et assurances, tout en menaçant les systèmes cryptographiques qui protègent aujourd'hui les transactions et données clients. Face à ces enjeux, le Forum des Compétences a dédié son groupe de travail 2025 au quantique, réunissant ses membres pour explorer collectivement les impacts technologiques, cyber et organisationnels sur le secteur financier, soit :

Risques du quantique

L'informatique quantique fragilisera à terme la cryptographie actuelle (RSA, ECC), rendant vulnérables les communications sécurisées, les données sensibles et les infrastructures critiques du système financier mondial. ⚠️

Opportunités du quantique

L'informatique quantique promet des gains significatifs en optimisation de portefeuille, en simulation avancée et en intelligence artificielle, ouvrant la voie à de nouveaux modèles de gestion des risques et d'efficacité opérationnelle. 🚀

Ce livre blanc est le fruit des ateliers thématiques du groupe de travail. Il porte une vision partagée : celle d'un secteur financier qui doit dès aujourd'hui préparer sa transition vers un environnement hybride classique-quantique, en renforçant sa culture technologique, en structurant sa migration post-quantique et en maîtrisant les risques associés. Il propose une synthèse des connaissances essentielles et des recommandations pratiques pour aborder sereinement cette nouvelle ère.

Ce document s'inscrit donc dans une volonté commune de renforcer la sécurité, la compétitivité et la résilience du secteur financier français face aux avancées rapides du quantique.

Livre Blanc

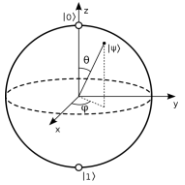
Thématique 1

Contexte général autour du quantique

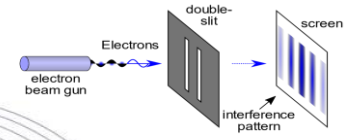
Acquérir les fondamentaux autour des technologies quantiques

Introduction aux technologies quantiques

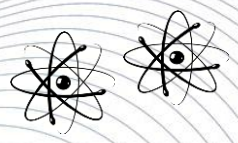
En exploitant les propriétés de la mécanique quantique…



Superposition Quantique



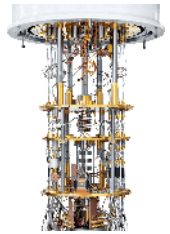
Interférence Quantique



Intrication Quantique

…on obtient les Technologies Quantiques

…en les appliquant sur des technologies actuelles…



Ordinateur quantique

Offrir une accélération des calculs

Communication quantique

Sécurité théorique de l'information

Capteurs quantiques

Capteurs avec haute précision

Les technologies quantiques reposent sur des phénomènes propres à la mécanique quantique, tels que la superposition, l'interférence ou l'intrication. Exploitées dans des dispositifs informatiques, de communication ou de détection, ces propriétés permettront d'atteindre, à maturité, des performances et des capacités difficilement accessibles avec les technologies classiques.

Elles ouvriront ainsi la voie à des calculateurs spécialisés capables d'accélérer certains traitements, à des communications dont la sécurité s'appuie sur les lois de la physique, et à des capteurs offrant une sensibilité accrue. Ensemble, ces trois domaines constituent les technologies quantiques modernes, dont les usages, les opportunités et les risques auront un impact croissant sur les principaux secteurs, dont le secteur financier.

Essentiel de l'informatique quantique

L'informatique quantique exploite les propriétés de la mécanique quantique pour réaliser des calculs à l'aide de particules physiques (atomes, ions, photons, électrons) servant de supports aux qubits. Contrairement au bit classique, limité à 0 ou 1, un qubit peut se trouver en superposition d'états, ouvrant la voie à des gains potentiels pour certains calculs spécialisés.

Tous les qubits ne se valent toutefois pas : stabilité, rapidité, précision et passage à l'échelle varient selon la technologie utilisée. Identifier l'architecture qui offrira le meilleur compromis entre performance et scalabilité reste l'un des grands défis de la course au calcul quantique. Les principales approches sont résumées dans le tableau ci-dessous.

*startups quantiques Françaises

Architecture	Principe	Acteurs principaux	Avantages	Défis	Niveau de maturité
Qubits supraconducteurs	Circuits supraconducteurs à très basse température	**Alice & Bob**, IBM, Google, Rigetti, Quantinuum	Vitesse d'opération élevée, industrialisation avancée	Températures proches du zéro absolu	🟩 **Avancé** (prototypes >100 qubits)
Atomes neutres	Atomes piégés par laser et manipulés par la lumière	**Pasqal**, QuEra, ColdQuanta	Scalabilité élevée, réseau reconfigurable	Complexité de manipulation et stabilité optique	🟧 **En développement** (dizaines de qubits)
Ions piégés	Ions chargés piégés par champs électromagnétiques	IonQ, Quantinuum, AQT, **Crystal Quantum**	Qubits très stables, haute fidélité d'opération	Opérations plus lentes que les supraconducteurs	🟩 **Avancé** (réseaux de 20–30 ions)
Photonique	Utilisation des photons comme porteurs de qubits	Xanadu, PsiQuantum, Quix, **Quandela**	Fonctionne à température ambiante, intégration sur puces optiques	Manipulation et détection des photons complexes	🟧 **Émergent** (petits prototypes)
Spin du silicium	Qubits basés sur le spin des électrons dans le silicium	Intel, Silicon Quantum Computing, Delft Univ., **CEA/Quobly**	Compatible avec les technologies CMOS	Contrôle individuel et lecture encore complexes	🟥 **Recherche active** (petits systèmes)

Actualité et évolution de l'informatique quantique

L'informatique quantique connaît aujourd'hui des avancées rapides, portées par des progrès technologiques majeurs, des stratégies nationales ambitieuses, un marché en pleine structuration, mais aussi des défis majeurs qu'il faudra surmonter pour permettre son développement futur.

Avancées technologiques

Les progrès récents du calcul quantique se traduisent par une augmentation régulière du nombre de qubits, certains prototypes dépassant désormais les 1000 qubits selon les architectures. Si l'avantage quantique reste limité à des cas d'usage spécifiques, la dynamique des avancées matérielles et logicielles montre une progression constante vers des systèmes plus performants et mieux maîtrisés.

Enjeux Stratégiques

L'informatique quantique est devenue un sujet stratégique pour les grandes puissances, comme en témoignent les nombreux plans nationaux et les investissements publics et privés, qui visent à structurer la recherche, l'innovation et l'adoption future de ces technologies. En France, près de 1,8 milliard € ont déjà été engagés depuis 2021, illustrant l'importance accordée à ce secteur émergent.

Marché Emergent

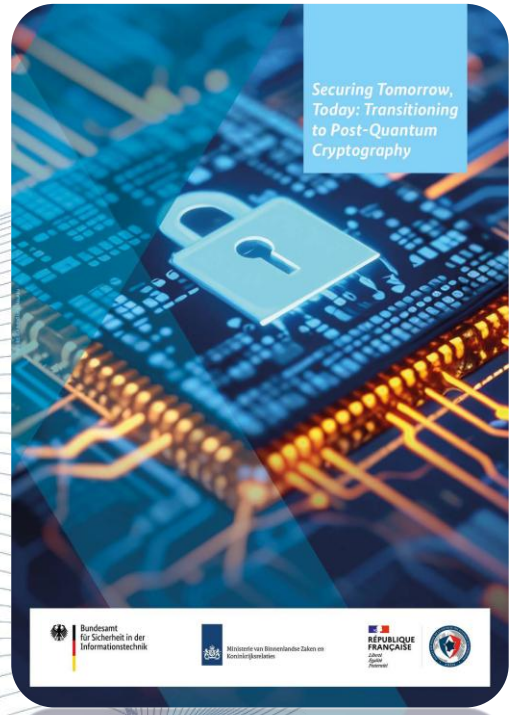
Le marché de l'informatique quantique reste modeste, estimé à environ 1,1 milliard € début 2025. Mais les projections sont ambitieuses : certaines études prévoient entre 8,7 et 13 milliards € d'ici 2035. Cette croissance serait portée par l'essor des technologies quantiques, les pilotes sectoriels et les premières applications concrètes.

défis Majeurs

Plusieurs défis subsistent, notamment l'identification d'une architecture dominante parmi les technologies actuelles. La capacité à produire des qubits fiables et en très grand nombre demeure un enjeu essentiel, tout comme la scalabilité des systèmes et l'interconnexion de futurs processeurs quantiques, nécessaires pour dépasser le stade des prototypes.

Aperçu des risques de l'informatique quantique

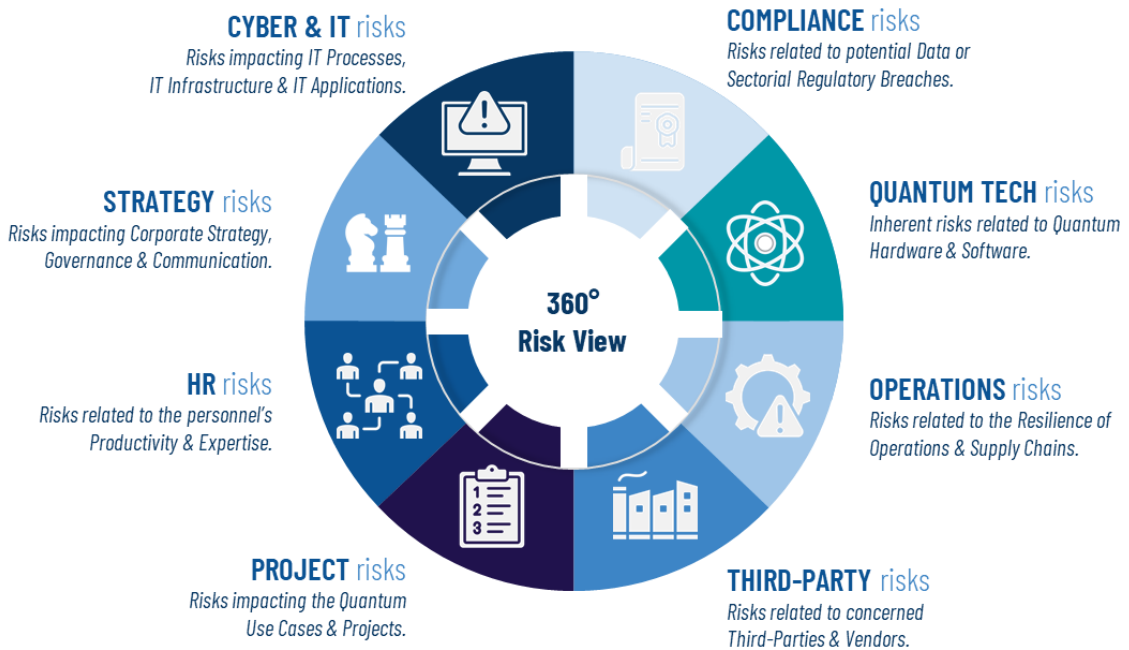
Cybermenace Quantique et Migration PQC



Les risques liés au quantique se répartissent en deux grandes catégories :

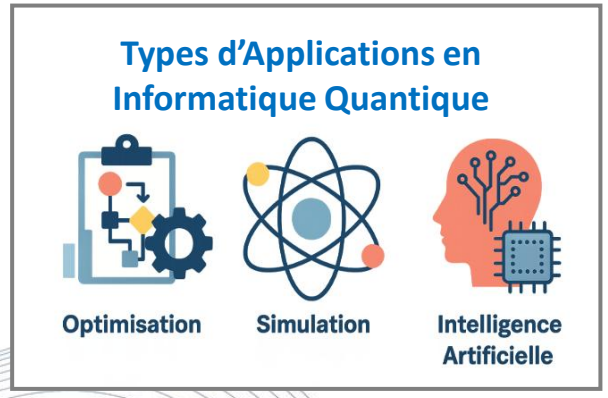
1. La cybermenace quantique, qui fragilisera les systèmes de chiffrement actuels et impose de préparer dès maintenant la transition vers la cryptographie post-quantique (détaillée dans la thématique 3 du livre blanc).
2. Les risques liés à l'adoption du quantique, moins visibles mais tout aussi importants, incluant les risques technologiques, organisationnels, réglementaires ou opérationnels qui accompagnent les nouveaux usages. (détaillée dans la thématique 6 du livre blanc).

Risques à Traiter lors de l'adoption du Quantique



Source: QRMF de QuRISK

Aperçu des opportunités de l'informatique quantique



Les applications de l'informatique quantique se répartissent en trois grandes catégories. L'**optimisation** permet d'aborder des problèmes complexes impliquant de nombreuses variables. La **simulation** exploite les propriétés quantiques pour modéliser précisément des phénomènes physiques, chimiques ou biologiques. L'**intelligence artificielle** quantique, enfin, cherche à accélérer certaines tâches d'apprentissage automatique grâce aux capacités des qubits.

*Les opportunités du quantique sont détaillées dans la **thématique 4** du Livre blanc.*

Ces trois catégories d'applications constituent aujourd'hui les principaux axes de développement du calcul quantique, et ouvrent la voie à des cas d'usage concrets dans de nombreux secteurs que l'on peut illustrer par les exemples suivants:

- **Optimisation : Optimisation de portefeuille**
  - Utiliser un algorithme quantique pour identifier la meilleure allocation d'actifs sous contraintes multiples (risque, liquidité, diversification).
  - Permet d'obtenir en quelques secondes des configurations qu'un algorithme classique mettrait des heures à explorer.
- **Simulation : Modélisation moléculaire avancée**
  - Simuler de manière précise des molécules complexes pour accélérer la découverte de nouveaux matériaux ou médicaments.
  - Le quantique permet de modéliser des interactions impossibles à reproduire avec des calculateurs classiques.
- **Intelligence Artificielle : Détection d'anomalies (QML)**
  - Déployer un modèle de Quantum Machine Learning pour identifier des comportements atypiques dans des millions de transactions ou de logs.
  - Utile pour la détection de fraude, la cybersécurité ou la surveillance en temps réel.

Sensibilisation au quantique : un besoin croissant

La sensibilisation au quantique doit couvrir à la fois les opportunités et les risques liés à ces technologies émergentes. Elle ne concerne pas uniquement les experts techniques : toute l'organisation est impactée, du top management aux équipes métiers, IT, R&D et cybersécurité. C'est pourquoi les actions de sensibilisation et de formation doivent être adaptées au contexte de chaque organisation et personnalisées selon les différents publics.

Top management	Métiers/Business	Équipes innovation/R&D	Équipes informatiques	Équipes cybersécurité
Identifier les opportunités stratégiques et les risques pour l'organisation	Comprendre les futurs cas d'usage et préparer les cas d'adoption	Explorer les potentiels de disruption et anticiper les nouveaux usages et modèles	Évaluer les impacts sur les infrastructures et l'intégration des nouvelles technologies	Anticiper les vulnérabilités, préparer la migration vers la cryptographie post-quantique

Objectif de sensibilisation par acteurs

Veille quantique : un enjeu stratégique

La veille quantique est essentielle pour identifier à la fois les opportunités offertes par les avancées technologiques et les menaces liées à la rupture cryptographique et aux nouveaux risques cyber. Elle doit être menée sur plusieurs axes : suivre les progrès hardware et software, comprendre l'évolution du marché et des cas d'usage, anticiper la transition vers la cryptographie post-quantique, et surveiller l'émergence de nouvelles réglementations.

Axes clés de veilles technologiques et business

Avancées Technologiques	Marché et Adoption	Migration PQC	Réglementations
Avancées hardware (nombre et stabilité des qubits, correction d'erreurs) et software…	Adoption de cas d'usage par secteurs industriels et performance des machines…	Protocoles et solution PQC, initiatives et PQC, programmes de migration PQC…	Réglementations sur l'informatique quantiques, la cybersécurité quantique et post-quantique…

Cette veille doit être à la fois technologique et stratégique, afin d'aider l'organisation à prendre des décisions éclairées et à préparer son adoption du quantique.

Messages clés de la thématique 1

Messages clés

- ✓ Les **Technologies Quantiques** ont donné naissance à trois grands domaines : **l'Informatique Quantique** (Quantum Computing), **la Communication Quantique** (Quantum Communication) et **les Capteurs Quantiques** (Quantum Sensing).
- ✓ Les ordinateurs quantiques progressent rapidement vers des architectures plus stables et plus scalables.
- ✓ Les principales **applications de l'informatique quantique: l'Optimisation**, **la Simulation** et **l'IA Quantique**.

En résumé

- ✓ Plusieurs architectures sont en compétition pour améliorer la fidélité, le passage à l'échelle et la stabilité des qubits (aujourd'hui 100~1 000 qubits sur les systèmes avancés).
- ✓ Les avancées de demain (ex. quelques milliers de qubits de meilleure qualité) **pourraient** permettre des avantages pratiques dans **certains cas d'usage spécifiques** avec des cas d'usage bouleversants pour la cryptographie prévu à partir de **1 million de qubits.**
- ✓ Le quantique comporte aussi **des risques** : adoption complexe, perte d'avantage en cas de retard, et **menace sur la cryptographie actuelle.**
- ✓ **Nécessité de sensibiliser** l'organisation et de maintenir une veille technologique et business structurée.

Livre Blanc

Thématique 2

Comprendre la cybermenace quantique

Appréhender la cybermenace quantique pour la cryptographie actuelle

Rappels sur les fondamentaux de la cryptographie

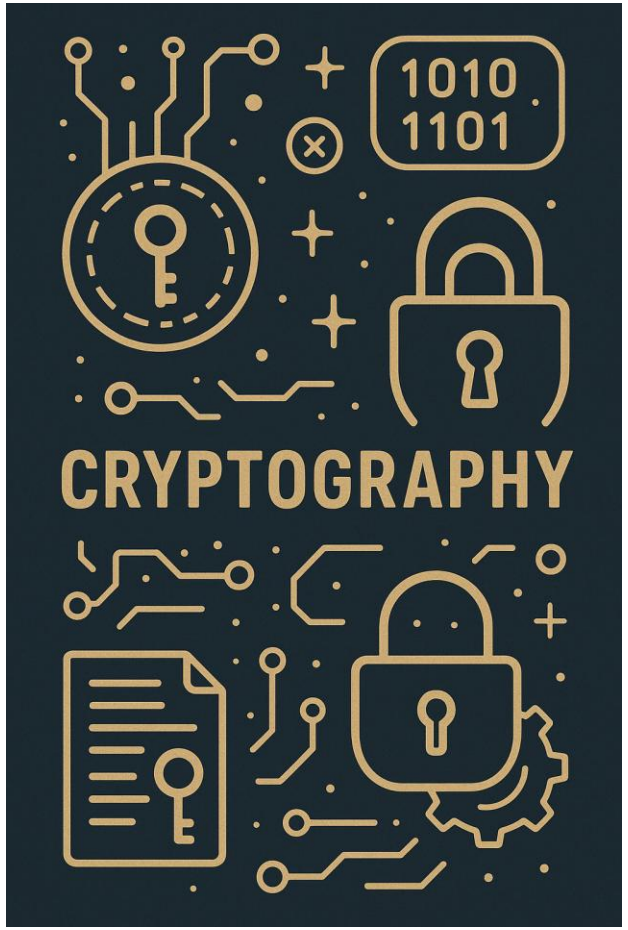
Qu'est-ce que la Cryptographie ?

La cryptographie est **l'art de protéger l'information** en la rendant illisible pour toute personne non autorisée. Imaginez-la comme un **coffre-fort numérique** : elle transforme vos données sensibles (mots de passe, transactions bancaires, messages privés) en un format incompréhensible pour les personnes malveillantes. La cryptographie regroupe des techniques qui permettent de garantir que les informations restent **confidentielles**, qu'elles ne sont pas **modifiées**, et que l'on peut **vérifier l'identité** des personnes ou des systèmes qui communiquent.

Dans notre monde connecté, la cryptographie protège quotidiennement :

- Vos paiements en ligne et opérations bancaires
- Vos emails et messages privés
- Vos mots de passe et identités numériques
- Vos communications professionnelles et personnelles

Sans cryptographie, il n'y aura pas de confiance numérique et internet tel que nous le connaissons n'existerait pas.



La cryptographie asymétrique

La cryptographie asymétrique : un système à double clé

La cryptographie asymétrique repose sur **deux clés différentes** : une clé publique (partagée) et une clé privée (secrète). Le principe est similaire à une **boîte aux lettres publique** où n'importe qui peut déposer un message, mais **seul le propriétaire possède la clé** pour l'ouvrir et consulter le message.

Elle permet de sécuriser les communications entre deux parties qui ne partagent pas de secret au préalable.

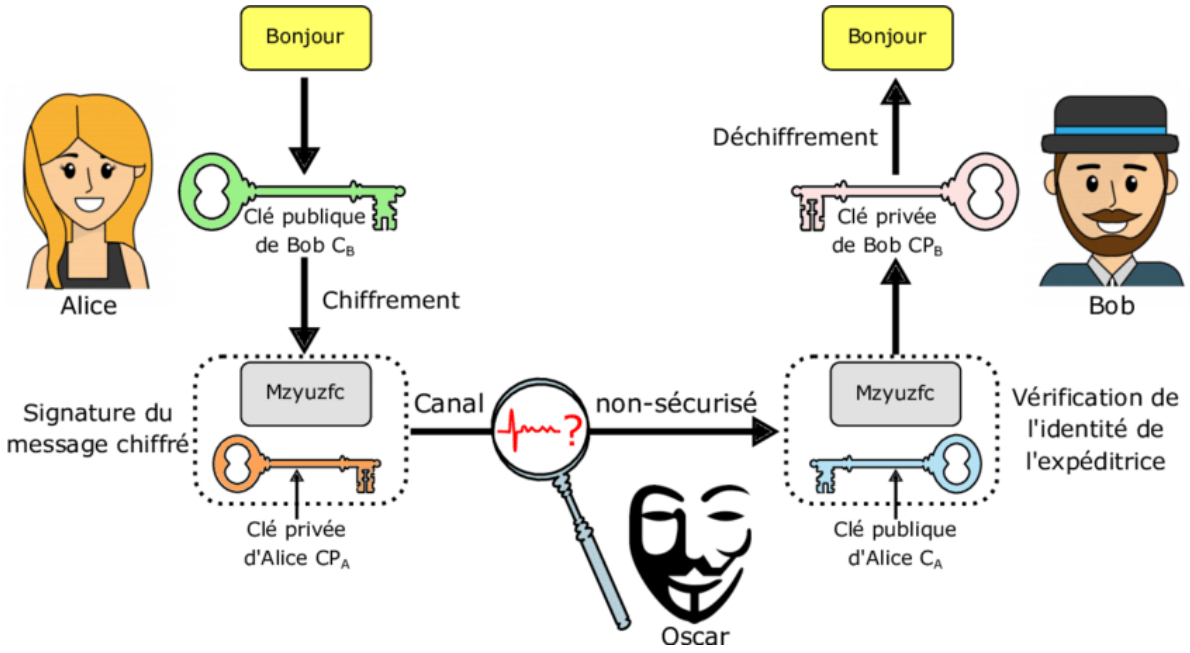
Méthodes courantes :

RSA: la plus utilisée historiquement

ECC: Courbes elliptiques (ECDH, ECDSA)

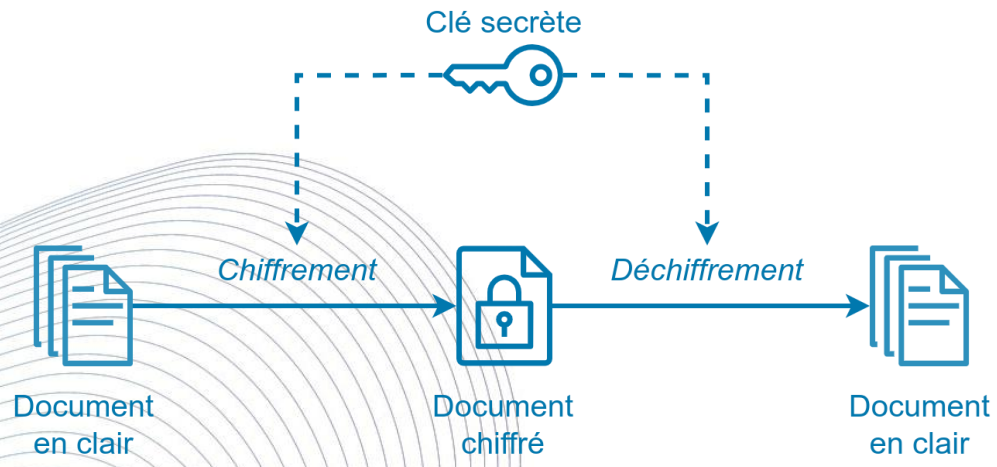
Diffie-Hellman (échange de clés)

Ces méthodes sont essentielles pour HTTPS, VPN, signatures électroniques et authentification, mais seront fragilisées par les futurs ordinateurs quantiques.



Source : Mathieu Dumont

La cryptographie symétrique



La cryptographie symétrique : un secret partagé

La cryptographie symétrique utilise **une seule clé secrète partagée** entre les deux parties. Elle est particulièrement rapide et efficace pour chiffrer de gros volumes de données ou des flux continus. Le principe est similaire à **cadenas classique** où l'expéditeur et le(s) destinataire(s) possèdent plusieurs exemplaires de **la même clé** pour fermer et ouvrir le message.

Méthodes courantes :

- AES (standard mondial, utilisé dans HTTPS, VPN, Wi-Fi, disques chiffrés)
- 3DES (ancien, progressivement retiré)
- ChaCha20 (rapide, utilisé dans TLS/HTTPS moderne)

Ces méthodes sont utilisées Protéger les communications après l'établissement d'une connexion sécurisée (ex: chiffrer des fichiers ou des disques durs). Cette famille de chiffrement reste solide face à la menace quantique, à condition d'utiliser des clés suffisamment longues (ex. AES-256).

Deux algorithmes quantiques, deux niveaux d'impact

Algorithme de Shor (1994)

Impact critique

Principe: Factorise les grands nombres premiers en temps polynomial, compromettant totalement la cryptographie asymétrique.

Impact: Rend obsolètes RSA, ECC et Diffie-Hellman. L'ensemble des infrastructures PKI, échanges de clés et signatures numériques sont vulnérables
→ **casser la cryptographie asymétrique**

Mitigation: Migration prioritaire et immédiate vers la cryptographie post-quantique. Le risque "Harvest Now, Decrypt Later" impose d'agir dès maintenant.

Algorithme de Grover (1996)

Impact modéré

Principe: Accélère quadratiquement la recherche exhaustive, réduisant de moitié la sécurité des clés symétriques.

Impact: Permet un brute-force efficace des clés : Une clé de 128 bits offre une sécurité équivalente à 64 bits face à un ordinateur quantique.
→ **Affaiblir la cryptographie symétrique**

Mitigation: Doubler la taille des clés (AES-128 → AES-256). Migration moins urgente mais à intégrer dans les feuilles de route.

Timeline de la cybermenace quantique

Ressources Nécessaires pour Compromettre RSA-2048: Selon les estimations scientifiques actuelles, la compromission de RSA-2048 via l'algorithme de Shor nécessiterait approximativement de 1 à 20 millions de qubits logiques stables avec correction d'erreurs quantique.

2024-2025

État de l'Art Actuel (2024-2025): Les systèmes quantiques les plus avancés (IBM Quantum System, Google Willow) disposent d'environ 1 000 qubits physiques. Ces qubits présentent encore des taux d'erreur importants nécessitant des mécanismes de correction d'erreurs qui multiplient significativement le nombre de qubits physiques requis pour un qubit logique.

2030-2035

Scénario optimiste (2030-2035) : Certains travaux de recherche suggèrent l'émergence possible d'un ordinateur quantique cryptographiquement pertinent (*CRQC - Cryptographically Relevant Quantum Computer*) dans cette fenêtre temporelle.

2035-2024

Scénario conservateur (2035-2040) : Les estimations plus prudentes situent cette échéance au-delà de 2035, en tenant compte des défis techniques liés à la stabilité des qubits et à la correction d'erreurs.

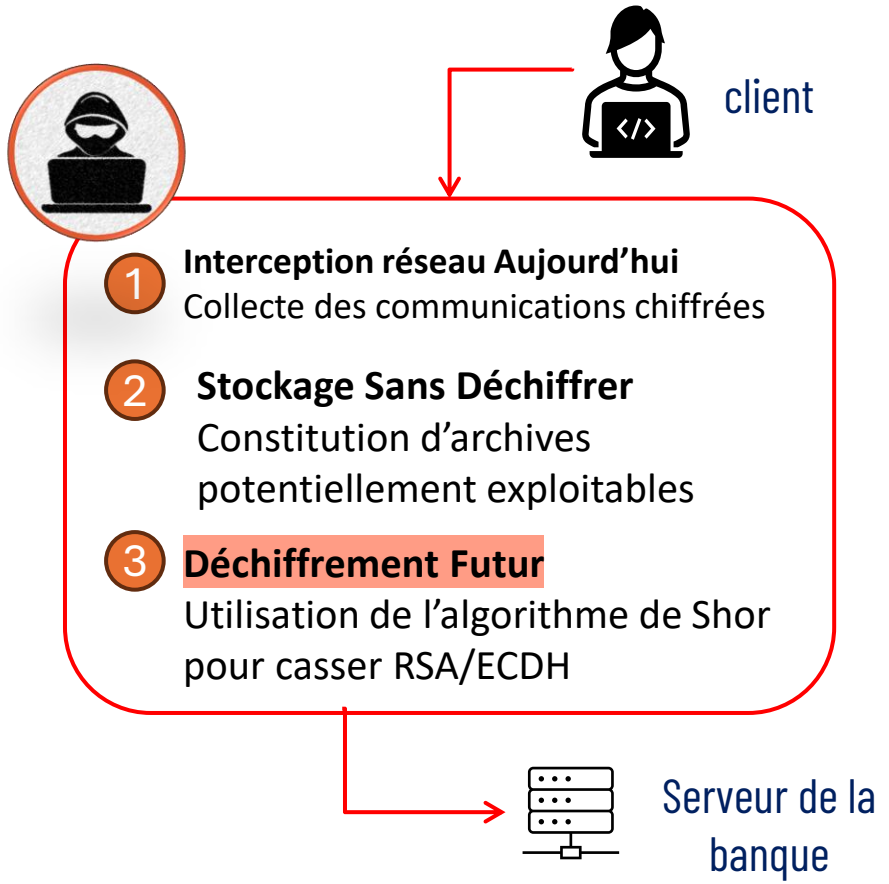
Incertitude technologique : L'absence de garantie quant à l'impossibilité de percées technologiques majeures impose l'application du principe de précaution. Par ailleurs, les méthodes algorithmiques progressent continuellement, réduisant les besoins en nombre de qubits.

« Harvest Now, Decrypt Later » : urgence d'Agir

Le concept « Harvest Now, Decrypt Later » (« Collecter maintenant, déchiffrer plus tard ») désigne une stratégie d'attaque anticipée qui exploite la menace des futurs ordinateurs quantiques.

Le principe de cette attaque s'articule en trois phases distinctes, Illustrées dans le schéma suivant.

Cette menace concerne particulièrement les données sensibles à durée de vie longue, (confidentialité à préserver au-delà de 10 à 15 ans): secrets industriels, dossiers médicaux, communications diplomatiques, ou encore informations personnelles et juridiques soumises à des obligations réglementaires strictes.



Du risque à la résilience: l'urgence d'agir

Les organisations disposent désormais de standards validés par NIST (présenté dans la thématique 3) pour initier leur migration cryptographique, avec des spécifications techniques complètes et des cas d'usage définis. La diversité des approches cryptographiques standardisées offre la flexibilité nécessaire pour adapter les stratégies de transition aux contraintes spécifiques de chaque environnement.

L'urgence d'agir découle d'une réalité simple : même si l'ordinateur quantique cryptographiquement pertinent n'existe pas encore, le risque est déjà présent à cause de l'attaque HNDL.

Le principe de précaution impose d'agir immédiatement sur les périmètres critiques afin d'adopter le **chiffrement post-quantique** de manière crypto-agile (expliqué en détails dans la thématique 3). Plus généralement, la crypto-agilité (facilité à faire évoluer les mécanismes cryptographiques déployés), constitue la réponse stratégique appropriée à cette menace émergente ainsi que les autres futures menaces cryptographiques.

Hiérarchisation de l'impact de la menace

La menace quantique ne frappe pas uniformément : les systèmes critiques manipulant clés, identités et transactions doivent être migrés en priorité absolue, tandis que les impacts varient selon l'urgence temporelle et la criticité métier.

Impact métier

PKI & Certificats: La chaîne de confiance repose sur les signatures RSA/ECDSA	**Transactions Financières:** Chiffrement (ECDH) et signatures (ECDSA) pour paiements	**Web banking & Apps:** Connexions HTTPS utilisent le TLS asymétrique pour l'échange de clé.
Applications Métiers: Schémas hybride RSA/AES	**VPN & Réseaux Internes:** ECDH/DH Tunnels IPsec/IKE utilisent Diffie-Hellman.	**Authentification (IAM, SSO, MFA):** Tokens JWT signés avec ECDSA, certificats client RSA.
TPE & Équipements IoT: Authentification/chiffrement basés ECC.	**Messagerie (S/MIME, PGP):** mails chiffrés avec clés publiques RSA/ECC.	**Signature Électronique:** Documents signés avec RSA/ECDSA

Urgence de migration

En complément de la **cybermenace quantique visant** les infrastructures IT du secteur financier, ce risque concerne directement l'univers **des crypto-actifs** : **les blockchains reposent largement sur la cryptographie asymétrique**, et celles, ainsi que leurs portefeuilles, qui ne migreront pas vers des primitives post-quantiques s'exposeront à un risque majeur de compromission, de vol d'actifs et de perte de confiance systémique.

Messages Clés de la Thématique 2

Messages clés

- ✓ Les algorithmes asymétriques **seront cassés** par l'ordinateur quantique; certains protocoles symétriques **seront affaiblis**.
- ✓ L'attaque « **Harvest Now, Decrypt Later** » rend urgentes les actions de protection des données à longue durée de vie **dès maintenant** **même si l'ordinateur quantique cassant RSA/ECC n'existe pas encore.**
- ✓ La réponse passe par la **Cryptographie Post-Quantique (PQC)**

En résumé

- ✓ La cryptographie asymétrique classique (RSA, ECC, DH…) sera **cassée**, la cryptographie symétrique sera **affaiblie mais renforçable**
- ✓ **Les SI sont tous concernés:**
  - ✓ les fondations de TLS, VPN, SSH, signatures, certificats sont affecté → l'infrastructure d'identité, d'authentification et de chiffrement
  - ✓ L'exposition touche à toute les couches dans le SI : **réseau**, **systèmes**, **applications**
- ✓ **Votre exposition est forte si** : vous stockez **des données sensibles à longue durée**, utilisez de l'asymétrique ou **manquez de crypto-agilité.**

Livre Blanc

Thématique 3

Migrer vers une cryptographie post-quantique

Planifier une migration graduelle vers de la cryptographie post-quantique

Protéger les données d'aujourd'hui et de demain

Une réponse anticipée à la menace quantique : la cryptographie post-quantique, dite *PQC**

Face au risque "Harvest Now, Decrypt Later", le National Institute of Standards and Technology (NIST) a lancé dès 2016 un programme de standardisation de la cryptographie post-quantique.

Ce processus rigoureux, déroulé en quatre phases de sélection (2017-2025), a mobilisé la communauté cryptographique internationale pour identifier des algorithmes résistants aux attaques quantiques.
NIST a publié **trois standards FIPS (+ 4ème en cours)** couvrant les usages fondamentaux de la cryptographie asymétrique:

- **FIPS 203** standardise CRYSTALS-Kyber (basé sur la cryptographie sur réseaux euclidiens) pour l'échange de clés
- **FIPS 204** (CRYSTALS-Dilithium, réseaux euclidiens) et **FIPS 205** (SPHINCS+, fonctions de hachage)
- **FIPS 206** (FN-DSA, Schémas de signature basés sur les réseaux) ***[en cours]***

- Les organisations disposent désormais de standards validés pour initier leur migration cryptographique.
- La diversité des approches cryptographiques standardisées offre la flexibilité nécessaire pour adapter les stratégies de transition aux contraintes spécifiques de chaque environnement.

Post-Quantum Cryptography

La crypto-agilité et l'hybridation

La crypto-agilité et l'hybridation constituent aujourd'hui des briques essentielles : elles préparent et sécurisent la migration vers des signatures et échanges post-quantiques.

Crypto-agilité

Capacité d'un système à **changer rapidement d'algorithmes cryptographiques** (classiques ou post-quantiques) sans refonte majeure.

- ✓ Réagit aux vulnérabilités
- ✓ Facilite les mises à jour futures
- ✓ Essentielle face à l'incertitude sur les algos PQC

→ *Ex : remplacement rapide de RSA par Kyber dans un protocole modulable.*

Hybridation

Combinaison d'un **algorithme classique (RSA/ECC)** avec un **algorithme PQC (Kyber/Dilithium)** en même temps.

- ✓ Assure la sécurité même si l'un des deux échoue
- ✓ Maintient la compatibilité avec l'existant
- ✓ Prépare une transition progressive

→ *Ex : TLS hybride avec ECDH + Kyber pour l'échange de clés.*

⚠️ **À noter:**
La cybersécurité quantique ≠ cybersécurité post-quantique (PQC) : la première utilise le quantique, la seconde remplace (ou hybride) les algorithmes classiques vulnérables par des nouveaux algorithmes classiques

Evolution de la position de l'ANSSI sur le PQC

L'ANSSI considère désormais la menace quantique sur la cryptographie asymétrique comme un risque stratégique. Elle suit activement les travaux internationaux (e.g., NIST, ETSI) et encourage une approche prudente et progressive.

ANSSI 2022

Prise de conscience et prudence

- Reconnaissance de la gravité de la menace quantique à moyen/long terme, notamment à cause du risque Harvest Now, Decrypt Later.
- la PQC n'est pas encore pleinement mature pour le déploiement immédiat
- Approche **progressive** recommandée : expérimentation, veille, adaptation des systèmes.

ANSSI 2023

Structuration et préparation

- Préparer activement la transition vers la PQC, sans négliger les menaces classiques.
- Définir les conditions d'une migration maîtrisée, notamment via l'hybridation.
- Accompagner les premiers visas de sécurité ANSSI PQC (2024–2025).
- Mener des analyses et enquêtes sur la maturité PQC en France.

ANSSI & BSI 2024

Position européenne commune*

- Agir dès maintenant : la migration PQC devient une priorité.
- Déployer des solutions hybrides pour les premières étapes.
- Sécuriser les cas d'usage sensibles d'ici 2030 contre les attaques store-now, decrypt-later.

***PQC Joint statement ANSSI, BSI + 17 EU Cyber Authorties**

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf?__blob=publicationFile&v=5

Livre Blanc « Quantique & Cybersécurité »
Roadmap européenne sur la transition PQC

La Commission européenne a publié une **feuille de route pour accompagner la transition vers la cryptographie post-quantique (PQC)** dans toute l'UE.

Eléments clés présentés :

- ✓ Le scénario "store now, decrypt later" est réel : vos données chiffrées pourraient être compromises demain.
- ✓ Les systèmes critiques mettent des années à migrer. Attendre, c'est s'exposer à des délais intenables.
- ✓ La crypto-agilité devient une exigence réglementaire (NIS2, CRA, DORA…).

D'ici fin 2026
Plans nationaux et premières analyses de risque PQC

D'ici fin 2030
Migration des cas d'usage sensibles

D'ici 2035
Fin de transition pour les cas d'usage restants

EC.europa.eu

Les standards sur la migration PQC

Au-delà de la standardisation des algorithmes post-quantiques, plusieurs organismes internationaux ont publié des recommandations pour accompagner les organisations dans leur transition. Ces initiatives couvrent l'ensemble du cycle de migration et constituent un cadre de référence indispensable pour structurer les programmes de migration PQC.

Standards NIST (États-Unis)

SP 800-208 Stateful Hash-Based Signature Schemes
Schémas de signatures pré-migration

SP 800-131A Rev. 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths
Règles de transition cryptographique

IR 8105 Report on Post-Quantum Cryptography
lignes directrices pour les organisations

Migration White Paper recommandation pour l'approche hybride, l' inventaire et la crypto-agilité.

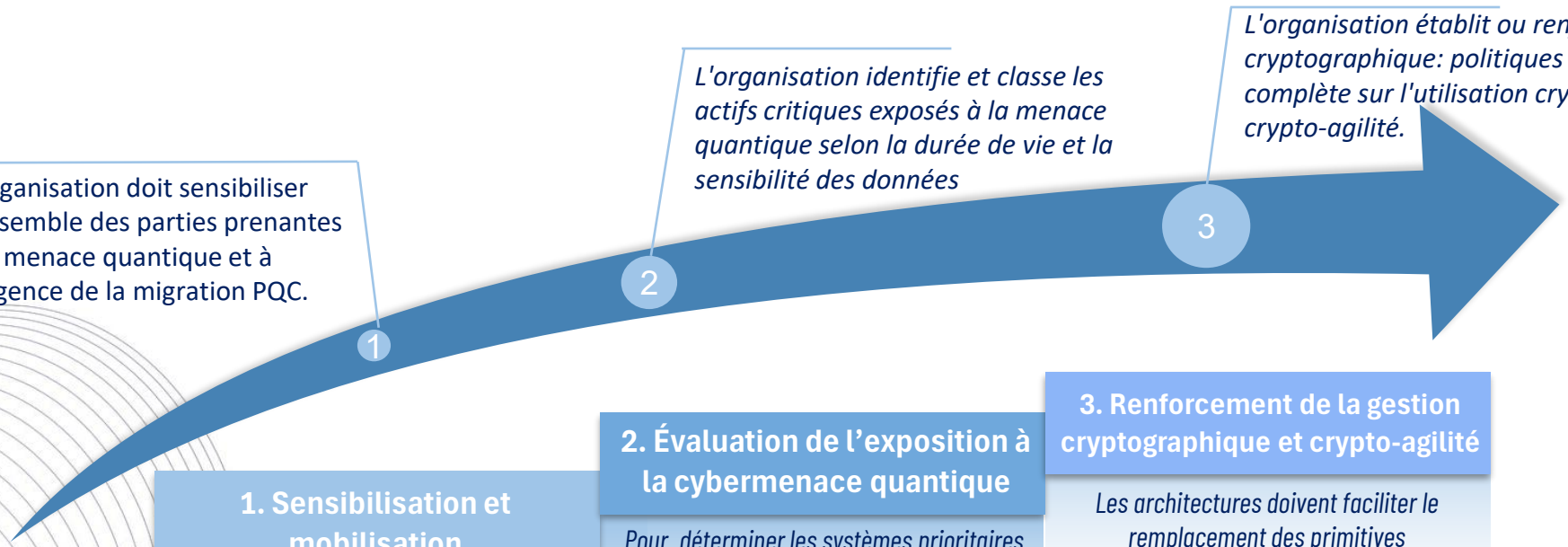
Spécifications ETSI (Europe)

TR 103 619 Migration Strategies and Recommendations
Schémas de signatures pré-migration

GR QSC 001 Agility and Migration Study
Crypto-agilité et bonnes pratiques

TS 103 744 Report on Post-Quantum Cryptography
Recommandations techniques opérationnelles

Migration PQC : étapes préliminaires



1. Sensibilisation et mobilisation

Cette étape inclut la formation des décideurs sur le risque "Harvest Now, Decrypt Later", et la sensibilisation adaptée par profil

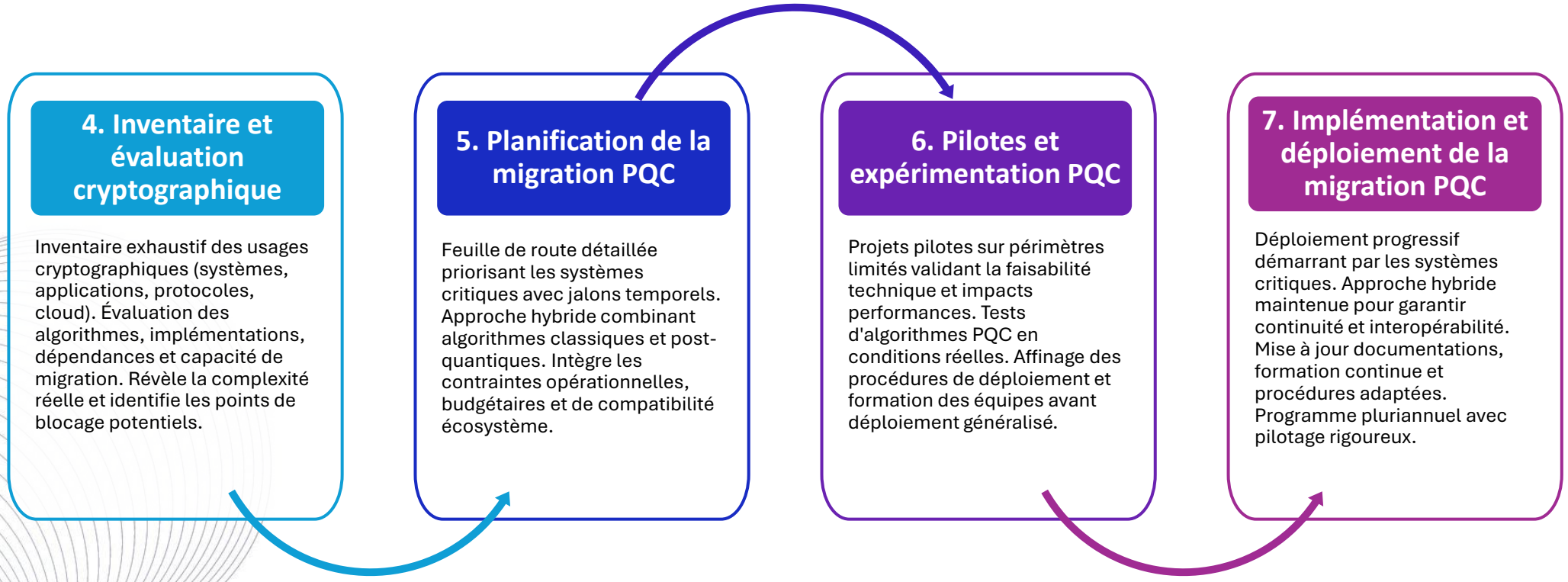
2. Évaluation de l'exposition à la cybermenace quantique

Pour déterminer les systèmes prioritaires nécessitant une protection immédiate, (informations confidentielles au-delà de 2030-2035). L'analyse porte sur la PKI, l'authentification et les communications sensibles, constituant le fondement de la stratégie de migration.

3. Renforcement de la gestion cryptographique et crypto-agilité

Les architectures doivent faciliter le remplacement des primitives cryptographiques sans refonte majeure, permettant une évolution rapide face aux menaces émergentes et aux évolutions normatives.

Migration PQC: de l'inventaire au déploiement



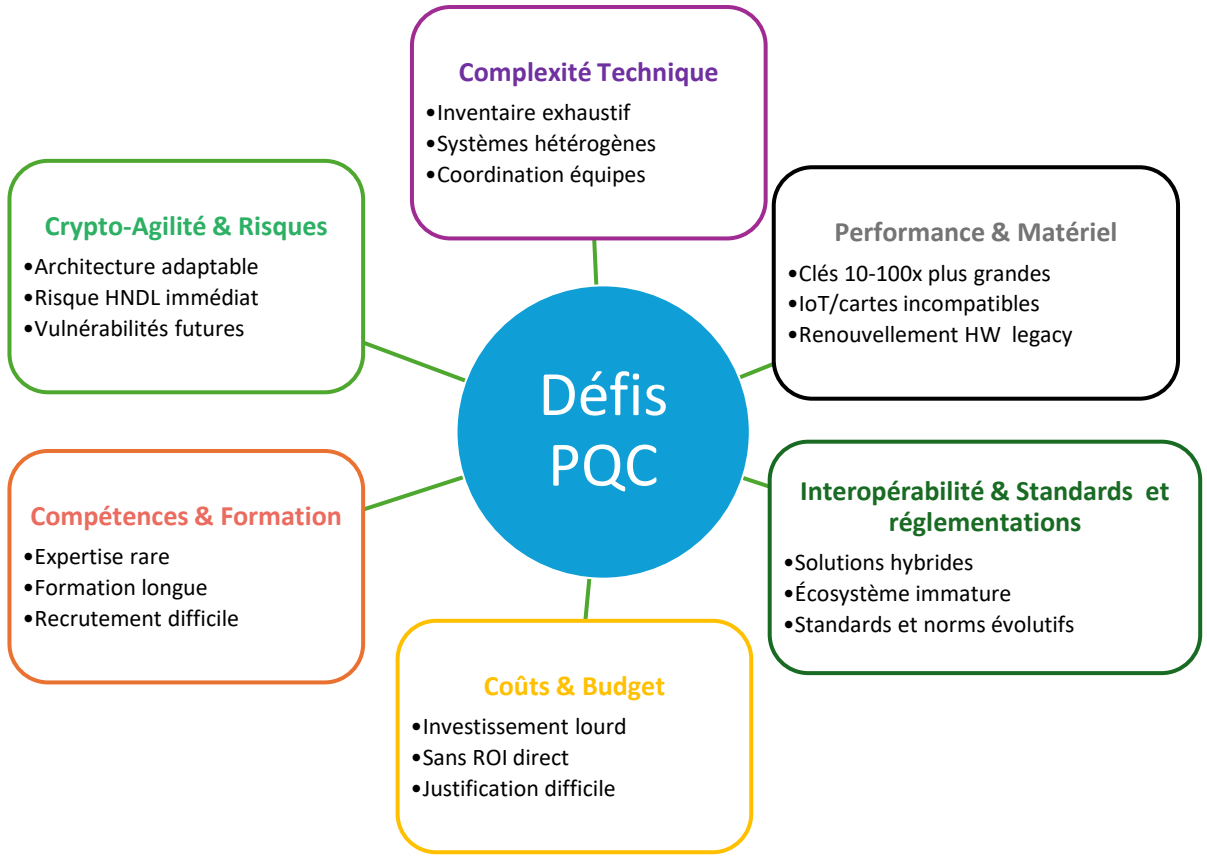
Challenges de la migration PQC

La migration vers la cryptographie post-quantique est un chantier majeur : elle requiert un programme de transformation pluriannuel, une gouvernance solide, des ressources dédiées, et un juste équilibre entre l'urgence imposée par la menace HNDL et la prudence liée à la maturité technologique.

Face à ces défis, la stratégie de réponse doit reposer sur:

- ✓ Approche hybride (classique + PQC) pendant la transition
- ✓ Priorisation par criticité : PKI et données longue durée d'abord
- ✓ Architecture crypto-agile pour adaptation future
- ✓ Formation continue et montée en compétence progressive

Vue 360 des défis de la migration PQC



Messages clés de la thématique 3

Messages clés

- ✓ La migration PQC est un projet **pluriannuel et complexe** qui nécessite une phase **de préparation** avant le **déploiement**.
- ✓ Les autorités européennes recommandent d'agir dès maintenant, les **standards**, **recommandations** (NIST, ETSI) et **réglementations liées** à la PQC évoluent rapidement imposant aux organisations de s'adapter en continu.
- ✓ La **crypto-agilité** devient un pilier essentiel : les architectures doivent permettre de **remplacer facilement les mécanismes cryptographiques** au rythme des **avancées technologiques.**

En résumé

- ✓ **La Phase 1 de la migration PQC - Préparation (2025-2027)** : Formation, allocation ressources, évaluation de l'exposition à la cybermenace quantique, renforcement gestion cryptographique et crypto-agilité.
- ✓ **Phase 2 de la migration PQC - Déploiement (2027-2030+)** : Inventaire cryptographique exhaustif, planification migration, pilotes PQC sur périmètres limités, implémentation progressive généralisée.
- ✓ Prioriser systèmes critiques et sensibles et suivre une approche hybride (classique + PQC) pendant la transition
- ✓ Face aux défis du projet, une **gouvernance cryptographique** forte et une **gestion de risques transversale** **est indispensable.**
- ✓ La Commission européenne a fixé (en juin 2025) l'objectif d'une **migration des actifs sensibles** d'ici **2030.**

Livre Blanc

Thématique 4

Les opportunités autour du quantique

Explorer les applications quantiques possibles (Use Cases)

Zoom sur l'informatique quantique

Un ordinateur quantique exploite les propriétés contre-intuitives de la physique quantique pour effectuer des calculs d'une manière radicalement différente des ordinateurs classiques. Là où un ordinateur classique manipule des bits (0 ou 1), un ordinateur quantique utilise **des portes quantiques** pour agir sur des **qubits** qui peuvent exister simultanément dans plusieurs états grâce à deux phénomènes fondamentaux :

L'Intrication quantique

- **Plusieurs qubits peuvent être "intriqués" : l'état de l'un dépend instantanément de l'état des autres, même à distance**

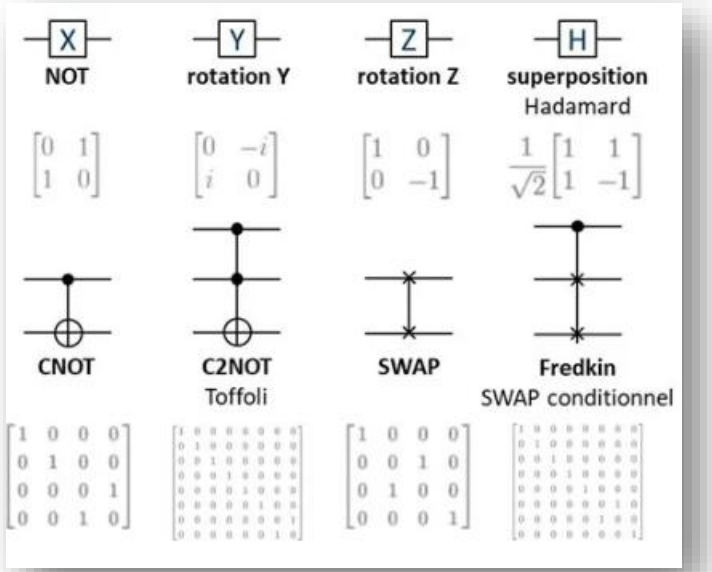
Exemple concret : Avec 3 bits classiques, on peut représenter un seul nombre parmi 8 possibilités (000 à 111). Avec 3 qubits en superposition, on peut représenter les 8 nombres simultanément. Avec 300 qubits, on pourrait représenter plus de possibilités qu'il n'y a d'atomes dans l'univers visible !

La superposition

- **Un qubit peut être dans l'état |0⟩, l'état |1⟩, ou les deux en même temps jusqu'à ce qu'on le mesure.**

Exemple concret : Imaginez un labyrinthe où au lieu d'explorer un chemin à la fois, vous pourriez explorer tous les chemins simultanément, et seul le bon chemin serait renforcé tandis que les impasses s'annuleraient d'elles-mêmes.

Représentation des portes quantiques



L'algorithmie quantique

Les portes quantiques constituent le paradigme dominant pour représenter et réaliser les opérations sur les qubits. Ces portes sont assemblées en circuits quantiques qui forment la base des algorithmes quantiques.

Les chercheurs ont développé une variété d'algorithmes quantiques exploitant ces circuits pour résoudre des problèmes spécifiques. Ces algorithmes se regroupent en plusieurs catégories selon leur objectif et leur impact sur différents domaines (dont la cybersécurité). Voici les principales familles et leurs représentants clés :

Fondamentaux	**Deutsch (1985)** Premier exemple d'avantage quantique théorique
	Deutsch–Jozsa (1992) Déterminer si une fonction est constante ou équilibrée
Recherche & optimisation	**Grover (1996)** Recherche non structurée en $O(\sqrt{N})$
	QAOA (2014) Optimisation combinatoire (hybride quantique-classique)
Cryptographie & sécurité	**Shor (1994)** Factorisation d'entiers, menace pour RSA/ECC
	Simon (1994) Précurseur de Shor, séparation exponentielle quantique/classique
Algèbre linéaire & ML	**HHL (2009)** Résolution rapide de systèmes linéaires
	Quantum PCA (2014) Analyse en composantes principales sur données quantiques
Simulation & physique	**Quantum Phase Estimation (QPE, 1995)** Estimation de phases/valeurs propres
	Quantum Fourier Transform (QFT) Transformée de Fourier quantique, base de Shor & QPE

Les applications de l'informatique quantique

L'informatique quantique représente une révolution technologique transversale dont les applications **touchent à plusieurs domaines**. Des services financiers à la santé, en passant par la logistique et l'énergie, cette nouvelle puissance de calcul ouvre des perspectives inédites dans tous les secteurs d'activité stratégiques.

Services financiers

- ✓ Optimisation de la gestion de portefeuille (quantum portfolio optimization).
- ✓ Détection avancée de fraudes grâce à des algorithmes d'apprentissage quantique.

Informatique et cybersécurité

- ✓ Optimisation de l'infrastructure de réseau (placement des antennes, routage intelligent).
- ✓ Détection des cyberattaques grâce à des algorithmes d'apprentissage quantique.

Logistique et transport

- ✓ Optimisation des itinéraires de livraison en temps réel.
- ✓ Gestion dynamique de flottes de véhicules autonomes.

Cas d'usage quantiques sur la cybersécurité

En plus des applications générales, il existe également des use-cases de l'informatique quantique qui utilise la communication quantique et les algorithmes quantique au service de la cybersécurité

1. Menaces quantiques

- **Rupture de la cryptographie asymétrique (RSA, ECC, DH)**
  → *Algorithme : Shor*
  → *Impact : nécessité de migrer vers la cryptographie post-quantique (PQC)*
- **Affaiblissement de certains hash et primitives**
  → *Algorithmes : Grover, Boneh–Lipton*
  → *Impact : augmentation de tailles de clés / durcissement crypto*

2. Opportunités pour la Cyberdéfense

- **Détection d'anomalies via Quantum Machine Learning (QML)**
  → Détection fine d'activités cyber anormales dans un SOC
- **Optimisation des défenses via QAOA**
  → Allocation optimale des ressources de sécurité (pare-feux, IDS/IPS)

3. Communication & transmission

- **Quantum Key Distribution (QKD)**
  → Sécurisation des communications très sensibles par génération de clés quantique
- **Quantum Random Number Generation (QRNG)**
  → Clés cryptographiques parfaitement aléatoires (VPN, TLS, banques)

RETEX cas d'usage quantiques (1/2)

HSBC : Trading Algorithmique Quantique (2024-2025)

Première mondiale en trading de bonds utilisant le processeur quantique IBM Heron combiné à des algorithmes classiques pour analyser 1 million de cotations sur 5 000 obligations européennes.

Résultat:

une amélioration de 34% de la prédiction de probabilité d'exécution des ordres au prix coté, surpassant les méthodes classiques seules dans l'extraction de signaux cachés dans les données de marché.

Cela prouve l'impact des algorithmes quantiques avec un avantage compétitif mesurable sur les marchés de gré à gré

Source: HSBC demonstrates world's first-known quantum-enabled algorithmic trading with IBM

AXA : Évaluation de Contrats d'Assurance et Modélisation des Risques (2022-2025)

AXA collabore avec Fraunhofer ITWM pour explorer le potentiel du quantique dans l'assurance, en particulier pour les simulations Monte-Carlo utilisées en valorisation de contrats et en calcul de capital économique.

Résultat:

L'algorithme d'estimation d'amplitude pourrait apporter une accélération quadratique à ces calculs intensifs, avec des bénéfices pour la modélisation des risques catastrophes naturelles, les stress tests VaR et l'optimisation de portefeuille.

Axa conclut que même si la technologie soit encore immature, commencer à comprendre et à développer des applications dès maintenant constitue la meilleure "police d'assurance" pour être prêt lorsque le matériel quantique atteindra sa maturité industrielle.

Source: Potential Applications of Quantum Computing for the Insurance Industry

RETEX use-cases quantiques (2/2)

Crédit Agricole CIB : Dérivés & Risque de Crédit (2021-2023, 2025)

Crédit Agricole CIB a mené plusieurs expérimentations quantiques avec Pasqal, Multiverse Computing puis Quandela sur deux cas d'usage majeurs : la valorisation de produits dérivés et la prédiction du risque de dégradation de crédit.

Résultat:

Les résultats ont démontré des gains de performance en calcul et en mémoire pour les modèles de pricing issus d'approches inspirées du quantique, et une qualité de prédiction équivalente à la production classique avec seulement ~50 qubits avec un potentiel d'amélioration significatif autour de quelques centaines de qubits.

Ces travaux confirment l'intérêt du quantique pour accélérer les calculs critiques en marchés de capitaux et améliorer la modélisation des risques financiers à horizon proche

Sources: Informatique quantique : résultats concluants de 2 expérimentations
Quantum innovation for finance: Crédit Agricole CIB and Quandela...

Messages clés de la thématique 4

Messages clés

- ✓ Les ordinateurs quantiques actuels restent limités, malgré une course mondiale pour améliorer leurs architectures.
- ✓ Les applications quantiques émergent déjà dans la finance, avec des use-cases concrets en algorithmique et en communication

En résumé

- ✓ Plusieurs organisations expérimentent déjà à travers des **pilotes** et des **use cases**. L'objectif est d'anticiper l'arrivée de l'ordinateur quantique en préparant les algorithmes et les use-cases dès maintenant.
- ✓ **L'algorithmie Quantique** repose sur l'utilisation **de portes** et **de circuits quantiques** permettant de concevoir **des algorithmes**, avec pour objectif de démontrer un véritable **avantage Quantique** par rapport au calcul classique.
- ✓ L'ordinateur quantique est considéré comme **un co-processeur.** Les instructions de operations quantiques sont envoyées à la puce quantique depuis un ordinateur classique.
- ✓ Il existe également **des algorithmes hybride** qui utilisent **le processeur quantique combiné à des algorithmes classiques**
- ✓ **En cybersécurité**, les **Use Cases** incluent le Quantum Machine Learning **(QML)** pour la cybersecurité, la distribution quantique de clés **(QKD)**, la génération de nombres aléatoires quantiques **(QRNG).**

Livre Blanc
Thématique 5

Gérer les risques de l’adoption du quantique

Assurer une gestion des risques efficaces lors des use cases quantiques

Rappel sur la gestion des risques technologiques

Le **risque** correspond à la combinaison entre la probabilité qu'un événement indésirable survienne et l'impact potentiel qu'il peut provoquer sur l'organisation.

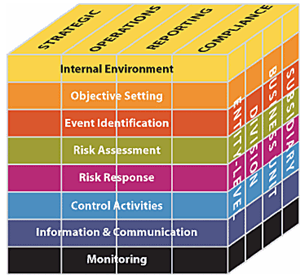
RISK = Likelihood x Impact

of undesired event — on organization

La **gestion des risques** consiste à identifier, analyser, traiter et suivre les risques susceptibles d'affecter l'organisation. Elle fournit un cadre structuré pour prioriser les menaces, guider les décisions et renforcer la résilience face aux enjeux technologiques et cyber.

ERM

31000
Risk Management



COSO ERM

IT & Cyber

AI

QRMF

QUANTUM

TECH RM

Plusieurs **standards** encadrent la gestion des risques, allant de cadres généralistes comme l'ISO 31000 à des Framework plus spécialisés pour l'IT ou les technologies émergentes, tels que l'IA ou le quantique.

La gestion des risques de l'adoption du quantique

Comme toute technologie avancée, **l'adoption de l'informatique quantique doit s'accompagner d'une gestion des risques structurée**, car la complexité des principes quantiques et l'immaturité actuelle de l'écosystème amplifient les incertitudes.

Pour sécuriser efficacement les projets quantiques, il est essentiel d'adopter **une approche multidimensionnelle couvrant l'ensemble des catégories de risques** (technologiques, organisationnels, opérationnels, humains, réglementaires ou liés aux tiers) et non de se limiter aux seuls risques techniques.

Cette **vision 360° garantit une analyse complète des menaces**, une meilleure anticipation des impacts et une transition plus maîtrisée vers les solutions quantiques.

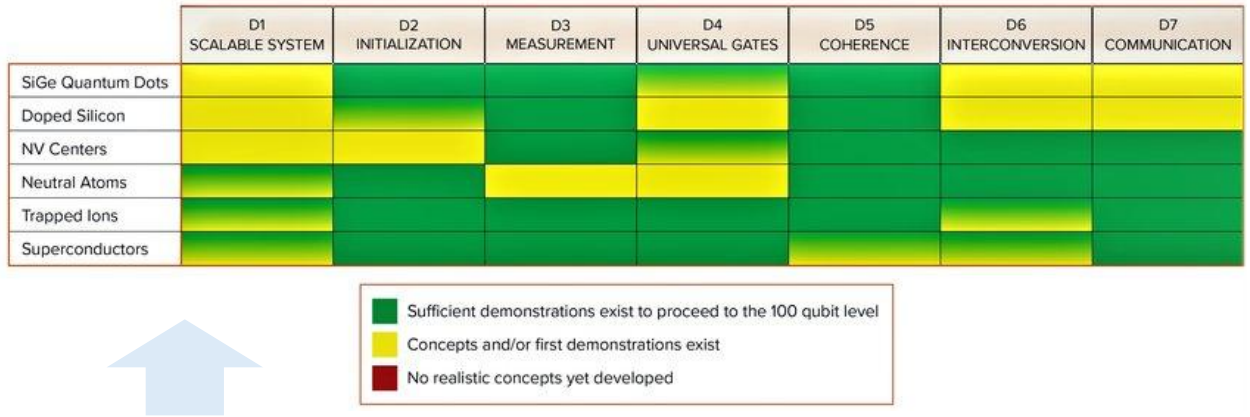
Source : Quantum Risk Management Framework (QRMF) - QuRISK

Risques liés à l'adoption de l'informatique quantique (1/2)

Même si le modèle proposé offre une vision large des risques liés aux projets quantiques, la catégorie des risques technologiques inhérents demeure l'une des plus critiques, car elle reflète directement la complexité scientifique, les limites physiques des qubits et la maturité encore progressive de ces technologies.

Voici quelques exemples de risques technologiques inhérents à l'informatique quantique :

- Maturité technologique insuffisante
- Erreurs et décohérence des qubits
- Évolutivité et interopérabilité limitées
- Dépendance technologique et souveraineté
- Manque de couche logicielle et d'abstraction
- Contraintes matérielles lourdes
- Incertitude sur la feuille de route technologique



Un des modèles les plus connus est le **critère de DiVincenzo**, qui définit les conditions nécessaires pour qu'un système quantique puisse effectuer un calcul fiable. Il offre ainsi un moyen structuré de suivre les limites actuelles des technologies quantiques et d'identifier leurs principales faiblesses.

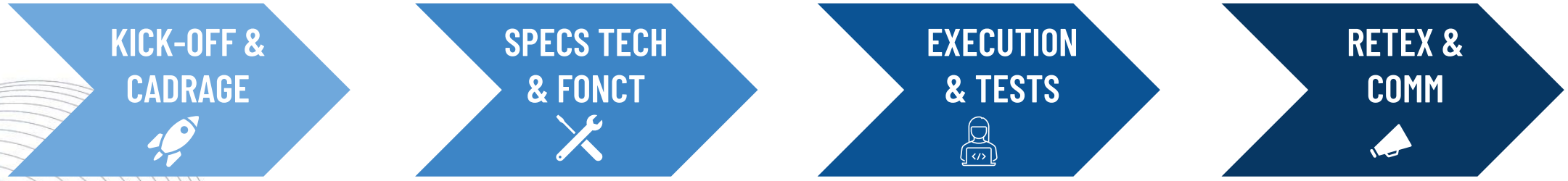
Risques liés à l'adoption de l'informatique quantique (2/2)

En complément des risques technologiques inhérents, l'adoption de l'informatique quantique expose les organisations à divers risques cyber, IT, stratégiques, humains, opérationnels ou liés aux fournisseurs. Une vision globale de ces dimensions est essentielle pour assurer une adoption maîtrisée. Voici quelques **exemples de scénarios de risques pour chacune des catégories** couvertes :

🛡️ Cyber Risk	💻 IT Risk	🎯 Strategy Risk	👥 HR Risk	🧩 Projet Risk	🤝 Vendor Risk	⚙️ Operations Risk
Exposition de données sensibles lors du traitement sur des plateformes quantiques cloud.	Difficulté d'interconnexion et d'intégration entre les environnements IT existants et la machine quantique.	Sélection de Use Cases à faible impact métier ou sans alignement clair avec les priorités stratégiques.	Manque de sensibilisation interne à la valeur et aux enjeux des expérimentations quantiques.	Mauvaise planification du cycle de vie du Use Case (objectifs flous, délais irréalistes).	Dépendance excessive à un fournisseur technologique (lock-in, modèle propriétaire).	Difficulté à reproduire ou fiabiliser les résultats des expériences quantiques.
Risque de fuite d'algorithmes ou de modèles quantiques lors du transfert ou du stockage.	Indisponibilité ou instabilité des services cloud supportant la plateforme quantique utilisée.	Surestimation du retour sur investissement ou de la maturité réelle de la technologie.	Dépendance excessive à un expert ou partenaire clé difficile à remplacer.	Absence de gestion continue des risques entraînant des dérives non maîtrisées.	Instabilité ou disparition d'un partenaire clé sur un marché encore émergent.	Manque de procédures de supervision et de résilience opérationnelle adaptées.

Gestion des risques et des projets quantiques

Une gestion de projet efficace repose toujours sur une maîtrise structurée des risques, et les projets quantiques ne font pas exception. Pour garantir une adoption sécurisée et maîtrisée, **la gestion des risques doit être intégrée à chaque étape** du cycle de vie d'un Use Case quantique. Voici un exemple illustrant comment articuler cette démarche tout au long du projet :



ETAPE PROJET	Phase initiale où sont définis les objectifs, périmètre, parties prenantes et les besoins.	Définition des exigences technico-fonctionnelles, de sécurité et interopérabilité du Use Case.	Phase d'expérimentation, de paramétrage et d'exécution des tests, pour valider les résultats.	Phase de retour d'expérience, d'analyse des résultats et de communication des conclusions.
ETAPE RISQUE	Identifier les risques clés pour cadrer le périmètre et orienter les choix technologiques.	Évaluer les risques techniques et data pour définir des exigences de sécurité adaptées.	Surveiller les risques opérationnels, d'ajuster le modèle et les résultats.	Analyser les incidents et écarts pour renforcer la maturité et améliorer les futurs Use Cases.

Défis et Importance de la Gestion des Risques Quantiques

La gestion des risques quantiques constitue encore un chantier émergent et souvent sous-estimé dans les phases d'expérimentation. Pourtant, l'arrivée progressive du quantique dans les organisations exige une approche plus structurée, évolutive et alignée avec les pratiques de gestion des risques technologiques. Comprendre les défis actuels et l'importance d'une démarche intégrée permet non seulement de sécuriser les initiatives quantiques, mais aussi d'en maximiser la valeur et la réussite.

Défis de la gestion des risques quantiques

- Souvent négligée en phase d'expérimentation.
- Approche statique et non évolutive si présente.
- Manque d'implication des experts risques.
- Manque de standards et référentiels QRMF.

Importance d'une approche risque intégrée

- Garantit une adoption sécurisée du quantique.
- Soutient l'innovation tout en maîtrisant les risques.
- Favorise le succès des expérimentations quantiques.
- Renforce la confiance des décideurs et des régulateurs.

Messages clés de la thématique 5

Messages clés

- ✓ La gestion des risques est indispensable dès les premières phases des projets quantiques.
- ✓ Une approche globale et multidimensionnelle est nécessaire pour maîtriser l'ensemble des risques.
- ✓ Une gestion des risques continue renforce la réussite, la sécurité et la crédibilité des expérimentations quantiques.

En résumé

- ✓ **La gestion des risques doit accompagner chaque étape** du Use Case quantique, même en phase d'expérimentation, pour anticiper les dérives et garantir la maîtrise du projet.
- ✓ **Une approche holistique est essentielle**, couvrant l'ensemble des dimensions : cyber, IT, stratégique, RH, conformité, opérationnelle et technologique, etc.
- ✓ **L'analyse des risques doit être proportionnée au niveau de maturité** et à l'étape **du Use Case**, afin de rester pragmatique, évolutive et orientée valeur.
- ✓ **La gestion des risques renforce la sécurité des projets d'adoption,** elle constitue aussi un levier de réussite et de crédibilité pour l'expérimentation quantique.
- ✓ **Intégrer la gestion des risques de bout en bout**, c'est créer les conditions d'une **adoption maîtrisée**, **durable** et **souveraine** des technologies quantiques.

Conclusion du
Livre Blanc « Quantique & Cybersécurité »

Conclusion

L'ère quantique marque une transformation technologique majeure dont les impacts toucheront simultanément l'innovation, la performance métier et la sécurité des systèmes d'information **du secteur financier**.

- **Contexte général :** Les technologies quantiques se structurent en trois domaines, calcul, communication et capteurs, et les progrès rapides des architectures de qubits confirment une trajectoire vers des systèmes plus stables, plus puissants et plus scalables.
- **Cybermenace quantique :** La capacité future de casser les algorithmes asymétriques, combinée à la menace Harvest Now, Decrypt Later, impose de protéger dès aujourd'hui les données sensibles et les communications critiques.
- **Migration post-quantique :** La transition sera progressive et pluriannuelle. Elle repose sur la montée en compétence, l'évaluation de l'exposition, la cartographie cryptographique, l'expérimentation de solutions hybrides et la priorisation des actifs critiques. Elle requiert crypto-agilité, gouvernance renforcée et gestion des risques transversale, en cohérence avec les orientations européennes et les standards NIST/ETSI, pour sécuriser les systèmes d'ici 2030.
- **Opportunités métier :** Les premières applications en optimisation, simulation et IA quantique ouvrent la voie à des gains concrets en finance, optimisation de portefeuilles, détection avancée de fraude, modélisation de risques, amélioration des algorithmes prédictifs.
- **Gestion intégrée des risques :** L'adoption des technologies quantiques doit s'appuyer sur une approche globale couvrant les axes cyber, IT, stratégiques, réglementaires, humains et opérationnels, afin de sécuriser les expérimentations et maximiser la valeur.

Se préparer à l'ère quantique, c'est protéger les fondations cryptographiques, anticiper les futurs usages et maîtriser les risques associés. Les organisations qui initient cette préparation dès aujourd'hui transformeront cette transition majeure en avantage stratégique durable.

Maitriser les risques et maximiser les opportunités

Soyez Prêts : l'ère du quantique commence Aujourd'hui !

Forum des Compétences

www.forum-des-competences.org