FORUM DES COMPÉTENCES
Cyber & Résilience

QuRISK
Quantum Risk & Cybersecurity

Colloque « Quantique & Cybersécurité »

11 décembre 2025

Quantum Risk Advisory (QuRISK)

www.qurisk.fr

Agenda

Introduction
« 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.

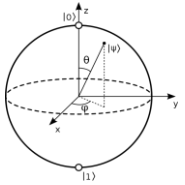
Thématique 1

Contexte général autour du quantique

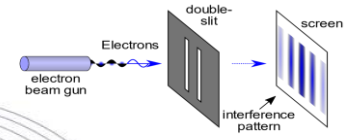
Acquérir les fondamentaux autour des technologies quantiques

Introduction aux technologies quantiques

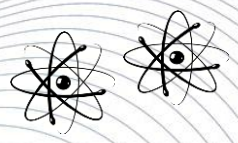
En exploitant les propriétés de la mécanique quantique…



Superposition Quantique



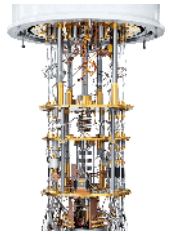
Interférence Quantique



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.

Messages clés de la thématique 1

- ✓ Les **Technologies Quantiques** trouvent leur fondement dans la mécanique quantique et ont donné naissance à trois grands domaines structurants : **l'Informatique Quantique** (Quantum Computing), **la Communication Quantique** (Quantum Communication) et **les Capteurs Quantiques** (Quantum Sensing).

- ✓ Les **ordinateurs quantiques progressent rapidement**, avec plusieurs architectures concurrentes fondées sur des supports physiques distincts (photons, atomes neutres, ions piégés, supraconducteurs, etc.), et devraient évoluer vers des architectures plus stables et plus scalables dans les prochaines années.

Thématique 2

Comprendre la cybermenace quantique

Appréhender la cybermenace quantique pour la cryptographie actuelle

Rappels sur les fondamentaux de la cryptographie

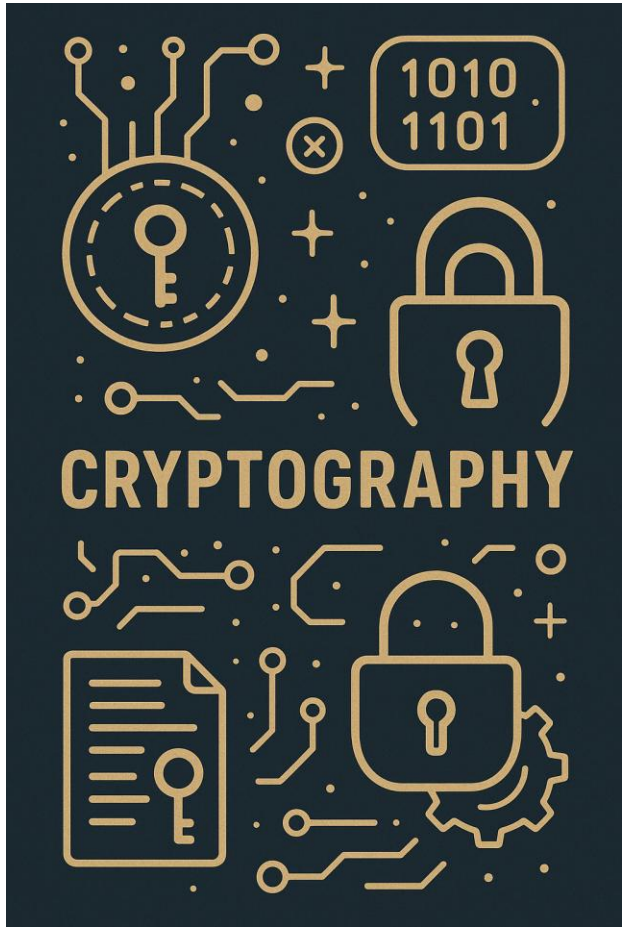
Qu'est-ce que la Cryptographie ?

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.



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.

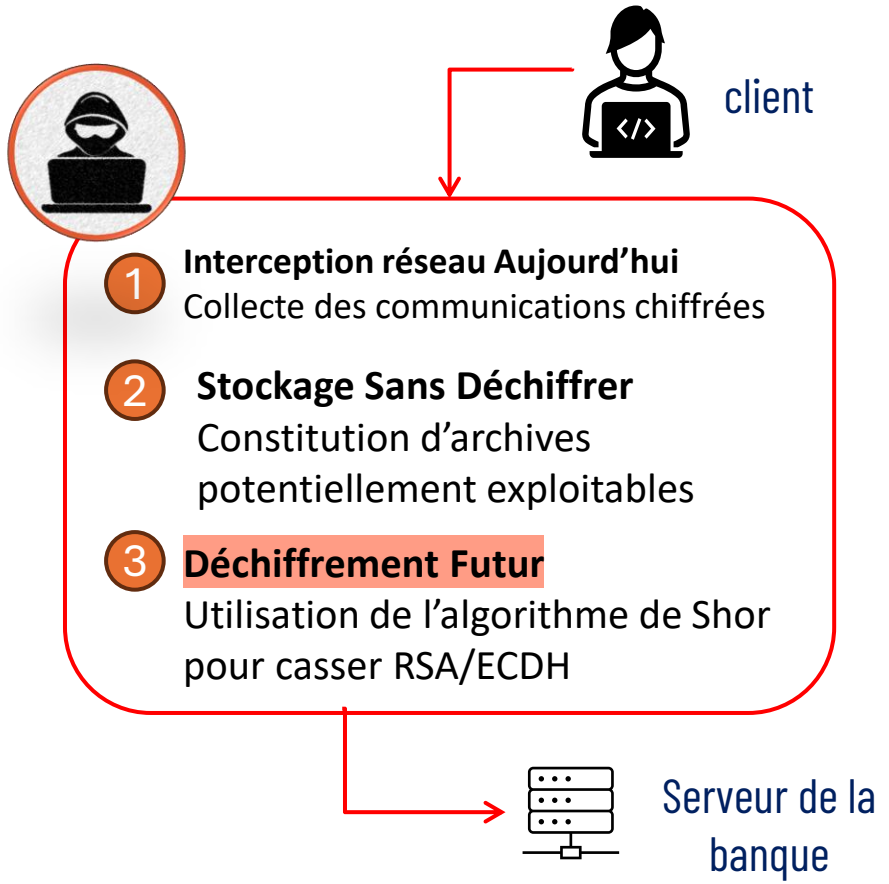
Incertitude technologique : L'absence de garantie quant à l'impossibilité de percées technologiques majeures impose l'application du principe de précaution. Par ailleurs, les méthodes algorithmiques progressent continuellement, réduisant les besoins en nombre de qubits.

« 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.



Messages Clés de la Thématique 2

- ✓ Les **algorithmes asymétriques actuels** seront **vulnérables face à l'ordinateur quantique**, notamment via l'algorithme de **Shor**, tandis que certains **algorithmes symétriques** verront leur **niveau de sécurité affaibli** par l'algorithme de **Grover**, nécessitant des tailles de clés plus élevées.

- ✓ La réponse repose sur une **transition** progressive vers la **Cryptographie Post-Quantique (PQC)**, impliquant l'adoption de **nouveaux protocoles résistants au quantique**, la mise à jour des systèmes et la préparation organisationnelle à une migration pluriannuelle.

- ✓ L'attaque **« Harvest Now, Decrypt Later »** consiste à intercepter et stocker aujourd'hui des données chiffrées, dans l'objectif de les déchiffrer ultérieurement, rendant la **migration PQC urgente** pour les organisations manipulant des **données sensibles à longue durée de vie**.

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

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

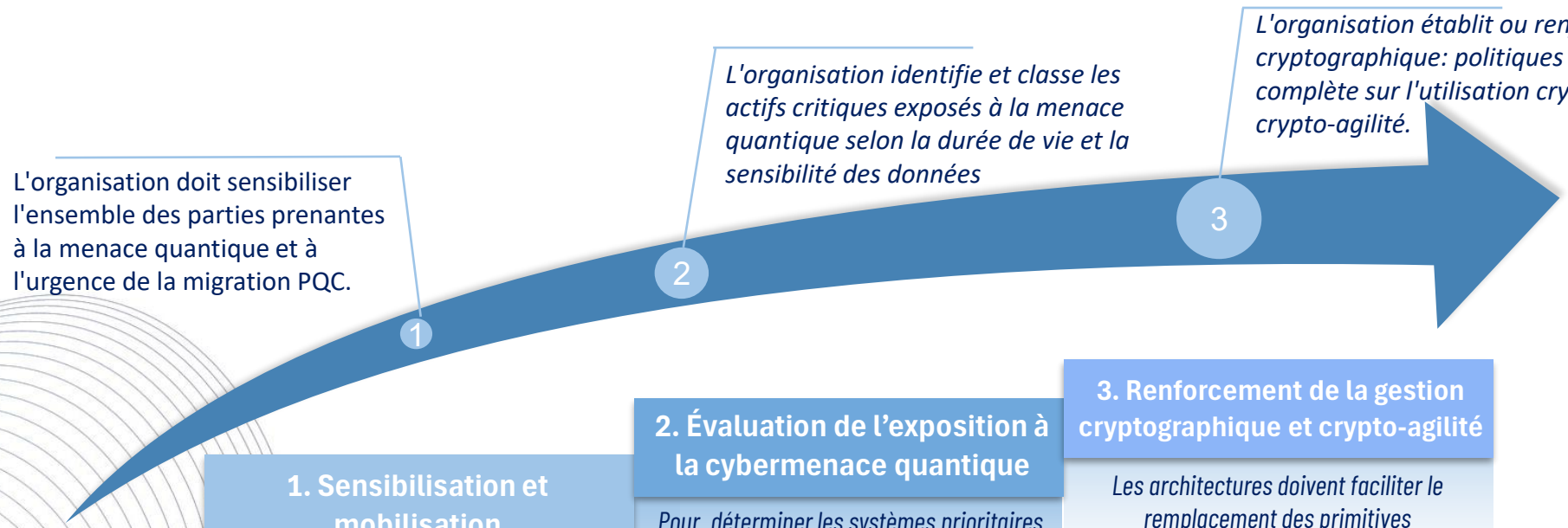
Migration des cas d'usage sensibles

D'ici 2035

Fin de transition pour les cas d'usage restants

EC.europa.eu

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

4. Inventaire et évaluation cryptographique

Inventaire exhaustif des usages cryptographiques (systèmes, applications, protocoles, cloud). Évaluation des algorithmes, implémentations, dépendances et capacité de migration. Révèle la complexité réelle et identifie les points de blocage potentiels.

5. Planification de la migration PQC

Feuille de route détaillée priorisant les systèmes critiques avec jalons temporels. Approche hybride combinant algorithmes classiques et post-quantiques. Intègre les contraintes opérationnelles, budgétaires et de compatibilité écosystème.

6. Pilotes et expérimentation PQC

Projets pilotes sur périmètres limités validant la faisabilité technique et impacts performances. Tests d'algorithmes PQC en conditions réelles. Affinage des procédures de déploiement et formation des équipes avant déploiement généralisé.

7. Implémentation et déploiement de la migration PQC

Déploiement progressif démarrant par les systèmes critiques. Approche hybride maintenue pour garantir continuité et interopérabilité. Mise à jour documentations, formation continue et procédures adaptées. Programme pluriannuel avec pilotage rigoureux.

Messages clés de la thématique 3

- ✓ La **Commission européenne a publié en juin 2025** une **feuille de route pour la transition PQC**, appelant les organisations à **évaluer leur exposition à la cybermenace quantique** d'ici fin 2026 et à **migrer tous leurs actifs critiques** vers des solutions résistantes au quantique avant fin 2030.

- ✓ Les principaux guides et **méthodologies de migration PQC** convergent vers une **approche progressive et fondée sur les risques**, intégrant la **sensibilisation**, des **évaluations des risques** et des impacts, un **inventaire des actifs cryptographiques**, les phases **d'expérimentation**, puis le **déploiement des protocoles PQC**.

- ✓ En parallèle des projets de migration PQC, **les organisations** doivent **améliorer leur gestion cryptographique** et **renforcer leur crypto-agilité**, afin de pouvoir adapter rapidement leurs mécanismes cryptographiques face à l'évolution des menaces, des standards et des exigences réglementaires.

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**

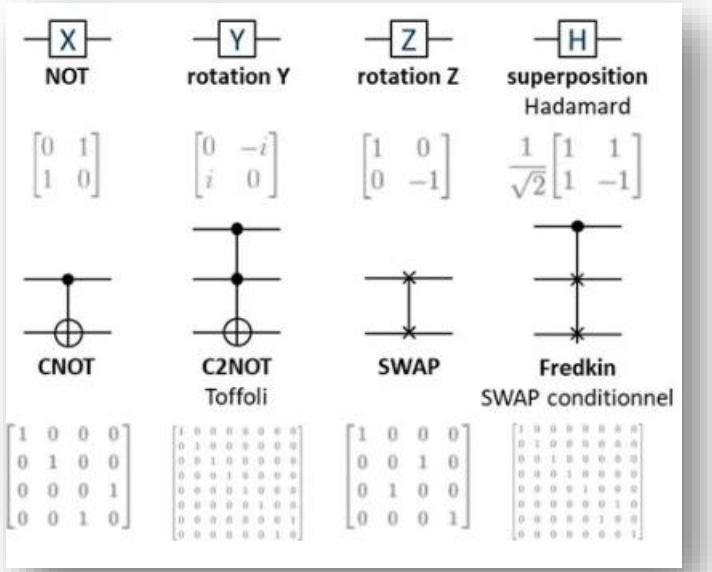
Exemple concret : Avec 3 bits classiques, on peut représenter un seul nombre parmi 8 possibilités (000 à 111). Avec 3 qubits en superposition, on peut représenter les 8 nombres simultanément. Avec 300 qubits, on pourrait représenter plus de possibilités qu'il n'y a d'atomes dans l'univers visible !

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



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)

Messages clés de la thématique 4

- ✓ Les principales **applications de l'informatique quantique** couvrent trois domaines majeurs : **l'optimisation**, **la simulation** et **l'intelligence artificielle quantique**.
- ✓ Dans le **secteur financier**, **plusieurs cas d'usage** émergent, notamment **l'optimisation de portefeuilles** financiers, **la détection d'anomalies** financière, **la simulation de scénarios** complexes (dont les simulations de Monte Carlo), etc.
- ✓ Les **technologies quantiques** peuvent également **renforcer la cybersécurité**, à travers des applications telles que le Quantum Machine Learning (**QML**) pour la détection d'anomalies cyber, la communication quantique sécurisée (**QKD**), et les générateurs quantiques de nombres aléatoires (**QRNG**) pour renforcer les mécanismes cryptographiques.

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.

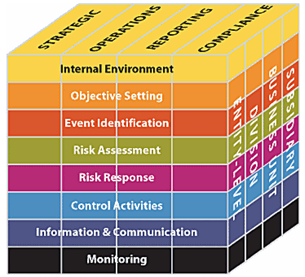
IT & Cyber

AI

QRMF

QUANTUM

31000
Risk Management



COSO ERM

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

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 :

	KICK-OFF & CADRAGE	SPECS TECH & FONCT	EXECUTION & TESTS	RETEX & COMM
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.

Messages clés de la thématique 5

- ✓ La **gestion des risques des projets quantiques** doit s'appuyer sur les bonnes pratiques existantes, adopter une **approche agile** et couvrir un **large spectre de dimensions**, au-delà des seuls risques technologiques (cyber, organisationnels, humains, réglementaires, fournisseurs, etc.).
- ✓ La **gestion des risques** doit être **intégrée à chaque étape du cycle de vie des projets quantiques**, de l'idéation à l'expérimentation puis au déploiement, et non traitée de manière ponctuelle ou « one-shot ».
- ✓ La **gestion des risques des initiatives quantiques** est nécessaire **dès les phases d'expérimentation**, même lorsque les cas d'usage sont encore éloignés d'une mise en production, afin de sécuriser les investissements et les trajectoires d'adoption.

Conclusion
« 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**. Voici les principales idées abordées dans cette présentation :

- **Les progrès rapides des technologies quantiques** (calcul, communication, capteurs) confirment une trajectoire vers des systèmes plus stables, plus puissants et plus scalables.
- **La cybermenace quantique impose d'agir dès aujourd'hui**, en particulier face aux risques sur la cryptographie actuelle et à la menace Harvest Now, Decrypt Later.
- **La migration vers la cryptographie post-quantique est progressive et pluriannuelle**, fondée sur la montée en compétence, les analyses et les inventaires, l'expérimentation et la priorisation du déploiement des actifs critiques conformément à la roadmap de l'UE.
- **L'informatique quantique ouvre des opportunités métier concrètes**, notamment en optimisation, simulation et intelligence artificielle quantique, avec **plusieurs cas d'usage émergents dans le secteur financier** et le domaine de la cybersécurité.
- **Une gestion des risques globale et continue constitue un facteur clé de succès,** couvrant l'ensemble des dimensions technologiques, cyber, réglementaires, humaines et opérationnelles.

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

Pour plus d'information,
télécharger notre livre blanc
« Quantique & Cybersécurité » :