



Comment Quantique

Ce que les administrateurs et
dirigeants doivent savoir à
l'ère quantique

Version française de "*Quantum How*" v1.2
Janvier 2026



Table des matières

01

**Franchir le seuil
quantique**

1.1 Cadrage exécutive

4

1.2 À propos de ce guide

6

02

**Ce que tout
dirigeant doit
savoir**

2.1 Les repères essentiels pour diriger

9

2.2 Votre appel à l'action (Boussole d'urgence)

10

2.3 Ce que vous devez savoir

13

2.4 Prochaines étapes immédiates pour les dirigeants

13

2.5 Questions clés à poser par les dirigeants

15

03

**Connaissances
additionnelles
pour les
dirigeants**

3.1 Adresser les questions les plus fréquemment posées

16

• 3.1.1 Q: Ordinateurs quantiques vs classiques : quelles différences ?

16

• 3.1.2 Q : Faut-il maîtriser la physique quantique pour comprendre le sujet ?

16

• 3.1.3 Q : Quelles industries tireront parti du calcul quantique ?

16

• 3.1.4 Q : Les ordinateurs quantiques remplaceront-ils les classiques ?

18

• 3.1.5 Q : Quels sont les risques liés à l'informatique quantique ?

18

• 3.1.6 Q : Qu'est-ce que la cryptographie post-quantique ?

19

• 3.1.7 Q : Qu'est-ce que la cryptoagilité, concrètement ?

20

• 3.1.8 Q : Quelle est la relation entre l'informatique quantique et l'IA ?

21

• 3.1.9 Q : Quelles capacités de calcul quantique sont disponibles aujourd'hui ?

22

• 3.1.10 Q : Quand les ordinateurs quantiques tolérants aux fautes arriveront-ils ?

22

• 3.1.11 Q : Quelle part est du bruit médiatique et quelle part est substantielle ?

22

• 3.1.12 Q : S'agit-il d'un nouveau moment Y2K ?

23

• 3.1.13 Q : Quelle est l'étendue de mon devoir fiduciaire ?

24

• 3.1.14 Q : Quelles nouvelles capacités mon organisation doit-elle développer ?

25

• 3.1.15 Q : Quel sera l'impact sur l'environnement ?

25

• 3.1.16 Q : Comment le Canada se situe-t-il par rapport aux autres pays ?

25

• 3.1.17 Q : Comment les pionniers créent-ils un avantage concurrentiel ?

25

• 3.1.18 Q : Pourquoi le secteur financier doit-il mener la transition quantique ?

26

• 3.1.19 Q : Pourquoi les standards sont-ils essentiels ?

27

• 3.1.20 Q : Pourquoi la souveraineté est-elle cruciale à l'ère quantique ?

27

• 3.1.21 Q : Peut-on expérimenter les technologies aujourd'hui ?

27

04 Votre feuille de route quantique

4.1 Principes directeurs	28
4.2 Années 0-1 : Posture de risque imminente	30
• 4.2.1 Rester informé en continu	30
• 4.2.2 Structurer pour réussir	31
• 4.2.3 Évaluer l'exposition aux risques et les échéanciers d'opportunités	33
• 4.2.4 Définir votre stratégie quantique défensive	33
• 4.2.5 Sécuriser les partenaires externes	34
• 4.2.6 Mettre en place le suivi des politiques et de la conformité	34
4.3 Années 1-2 : Expérimentation et montée en capacité	34
• 4.3.1 Développer votre stratégie quantique	34
• 4.3.2 Prioriser et financer votre stratégie	35
• 4.3.3 Bâtir pour le long terme	35
4.4 Années 3-5 : Avantage stratégique	35

05 Annexes et outils

5.1 Glossaire des termes	36
5.2 Notes explicatives sur des concepts sélectionnés	38
• 5.2.1 Autres technologies quantiques	38
• 5.2.2 Vue d'ensemble des risques	38
• 5.2.3 Types d'architectures de qubits	40
• 5.2.4 Fournisseurs canadiens d'ordinateurs quantiques	40
• 5.2.5 Internet des objets (IoT)	40
• 5.2.6 Questions clés supplémentaires pour les dirigeants	42
• 5.2.7 Panorama des normes	44
• 5.2.8 Advanced Cryptographic Concepts	45
5.3 Suppléments à ce guide	46
5.4 Références et apprentissage continu	47

06 Contributeurs et remerciements

Leaders d'opinion et endosseurs	48
Réviseurs experts et conseillers	49
Rédaction et production	49
À propos de l'auteure	49

1

1.1

Franchir le seuil quantique

Cadrage exécutive

“

Appel national à l'action : l'informatique quantique n'est plus une possibilité lointaine ; elle est une réalité imminente.

Lisez cette section pour saisir l'orientation du guide et optimiser le temps que vous y consacrez.

Au-delà des opportunités et menaces propres à chaque organisation, ce document vise à mobiliser l'ensemble des acteurs économiques autour d'une stratégie nationale. Le Canada possède l'un des écosystèmes quantiques les plus avancés au monde. Nous avons prouvé notre leadership. Il faut maintenant passer à l'échelle. Les secteurs gouvernemental, de la défense et le milieu universitaire se sont déjà engagés à soutenir cette ambition. Les industries canadiennes, en particulier le secteur financier, doivent maintenant s'aligner pour servir l'intérêt national et assurer le leadership technologique du Canada.

Pourquoi maintenant

- Les signaux de cette technologie transformationnelle sont clairs, mais trop d'organisations en ignorent le potentiel ou **restent dangereusement mal préparées**.
- Au moment où ces organisations réagiront, le quantique pourrait déjà avoir **profondément remodelé les paysages numérique, économique et géopolitique**.

Ce qu'est le quantique

- L'informatique quantique est une nouvelle classe de technologies informatiques fondée sur une **approche radicalement nouvelle de calcul**.
- L'informatique quantique nous permettra de résoudre des problèmes complexes qui sont **hors de portée des capacités de calcul** des technologies informatiques classiques.
- Son impact sera **transformationnel et systémique**, avec des retombées dans tous les secteurs.
- Du **côté positif**, elle élargira les frontières du savoir en permettant des percées en science, médecine, logistique, finance et science du climat.
- Du **côté sombre**, elle peut briser différentes normes de chiffrement¹ et d'authentification² actuelles et compromettre les **fondements de la confiance numérique mondiale**.

État actuel de l'informatique quantique

- Les ordinateurs quantiques de première génération **sont déjà en service**³, utilisés pour la recherche et comme bancs d'essai via des partenariats avec des acteurs industriels pionniers⁴.
- Un consensus croissant suggère que des ordinateurs quantiques tolérants aux fautes⁵ **pourraient émerger d'ici 2030**.

¹ Le chiffrement transforme l'information en une forme codée, accessible uniquement avec la clé de déchiffrement adéquate.

² L'authentification confirme qu'une personne, un appareil ou un système est bien celui qu'il prétend être, à l'aide de signatures numériques ou d'identifiants.

³ Les ordinateurs *Noisy Intermediate-Scale Quantum* (NISQ) permettent des usages expérimentaux ciblés, mais restent fortement exposés au bruit et aux erreurs.

⁴ Parmi les exemples bien documentés figurent JP Morgan, HSBC, Banco Santander, Merck, Johnson & Johnson, Roche, Amgen, Moderna, AstraZeneca, Sanofi, DHL, Volkswagen, BMW, Ford et Airbus, ainsi que la Banque du Canada. Voir l'annexe pour les liens vers « The Quantum Index ».

⁵ Un ordinateur quantique entièrement corrigé des erreurs, capable d'exécuter de manière fiable des calculs longs et complexes, marquant le seuil d'un usage commercial à grande échelle.

Pourquoi il faut agir

- L'informatique quantique apporte à la fois des opportunités transformatrices et des risques disruptifs; **en tant que dirigeants, nous devons nous préparer aux deux.**
- Les organisations qui se mobilisent tôt peuvent **capter les bénéfices** de cette nouvelle technologie et sécuriser un **avantage de premier arrivant**⁶.
- Parallèlement, l'informatique quantique introduit **des niveaux de risque systémique mondial intolérables**, exigeant une mobilisation immédiate pour les atténuer.
- Les organisations qui **tardent à agir** compromettent leur compétitivité et leur résilience, et contribuent aux **menaces mondiales sur la confiance numérique**, la stabilité des réseaux et la souveraineté technologique.

La finance en première ligne

- Le leadership individuel et collectif du secteur financier déterminera si l'ère quantique **débute dans la crise ou dans la confiance.**
- Compte tenu de leur infrastructure cryptographique, de leurs pratiques prudentielles et de leur rôle économique, **les banques sont les gardiennes naturelles de la confiance numérique.**
- La nature de leurs données et leur **importance systémique** pour les marchés les placent en première ligne des **cyberattaques quantiques précoces.**
- Les banques ont l'expertise. Ils entretiennent depuis longtemps un **lien étroit avec la physique**⁷ et **peuvent bénéficier directement et rapidement** des nouvelles capacités quantiques.
- Les banques disposent de **capacités de coordination mondiale** via des régulateurs expérimentés en matière de résilience.
- **Un alignement précoce des banques créerait un effet d'entraînement**, plusieurs autres industries s'alignant volontairement sur leurs échéanciers et leurs normes.

Le fossé de leadership

- Le leadership est une anticipation en action. Il consiste à **agir avant que les conséquences** ne deviennent inévitables.
- À mesure que la puissance quantique augmente, les **risques et coûts de redressement augmentent** pour ceux qui ne s'y préparent pas.
- Les **signaux sont clairs** et les enjeux sont majeurs ; les dirigeants ont une responsabilité fiduciaire d'agir. L'inaction deviendra rapidement une **défaillance fiduciaire.**
- Cependant, la complexité du quantique et l'ampleur de ses impacts rendent **difficile pour les dirigeants d'en saisir la portée.**
- Les dirigeants peuvent faire preuve d'audace et de courage, mais ils ne peuvent agir avec confiance et clarté sur ce qu'ils ne comprennent pas fondamentalement.

Comblé le fossé

- Un leadership responsable ne peut s'exercer que **lorsque les impératifs du quantique sont clairs.**
- **Une source fiable, claire et actionnable** est nécessaire pour combler le fossé entre compréhension et action du leadership.
- **Ce guide existe pour combler ce fossé.**



1.2

Ce guide donne aux dirigeants les connaissances essentielles pour guider leur organisation dans les premières étapes du paradigme quantique.

À propos de ce guide

Conçu pour les conseils d'administration et les dirigeants exécutifs, ce guide s'exprime dans le langage qui fonde vos décisions : **risque**, **confiance**, **échéancier**, **stratégie**, **surveillance** et **responsabilité**.

Langage non technique



En utilisant exclusivement un langage non technique, il rend les impératifs de l'informatique quantique immédiatement **compréhensibles et indéniablement clairs** pour les dirigeants.

Informations essentielles



Il rassemble l'information essentielle dont chaque conseil d'administration et équipe de direction a besoin pour agir avec clarté, le niveau **d'urgence approprié et confiance**.

Prochaines étapes et stratégie à long terme.



En exposant clairement les enjeux et en répondant aux questions clés du leadership, ce guide peut orienter à la fois vos prochaines **étapes immédiates et votre stratégie à long terme**.

Devoir fiduciaire et positionnement national.



Suivez-le pour assumer vos responsabilités fiduciaires, protéger la **souveraineté numérique** et maintenir la **position du Canada*** à l'avant-garde du quantique.

• Au Canada, le Québec se distingue comme un pôle majeur, ancré à Sherbrooke.

Ce guide est divisé en six sections.
Voici un aperçu et leur mise en action.

Comment a-t-il
été conçu ?

Ce guide a été élaboré et affiné à travers une vaste démarche collaborative impliquant l'industrie quantique, l'écosystème académique et la communauté d'affaires au sens large. La liste complète des collaborateurs et des appuis figure dans la section 6.

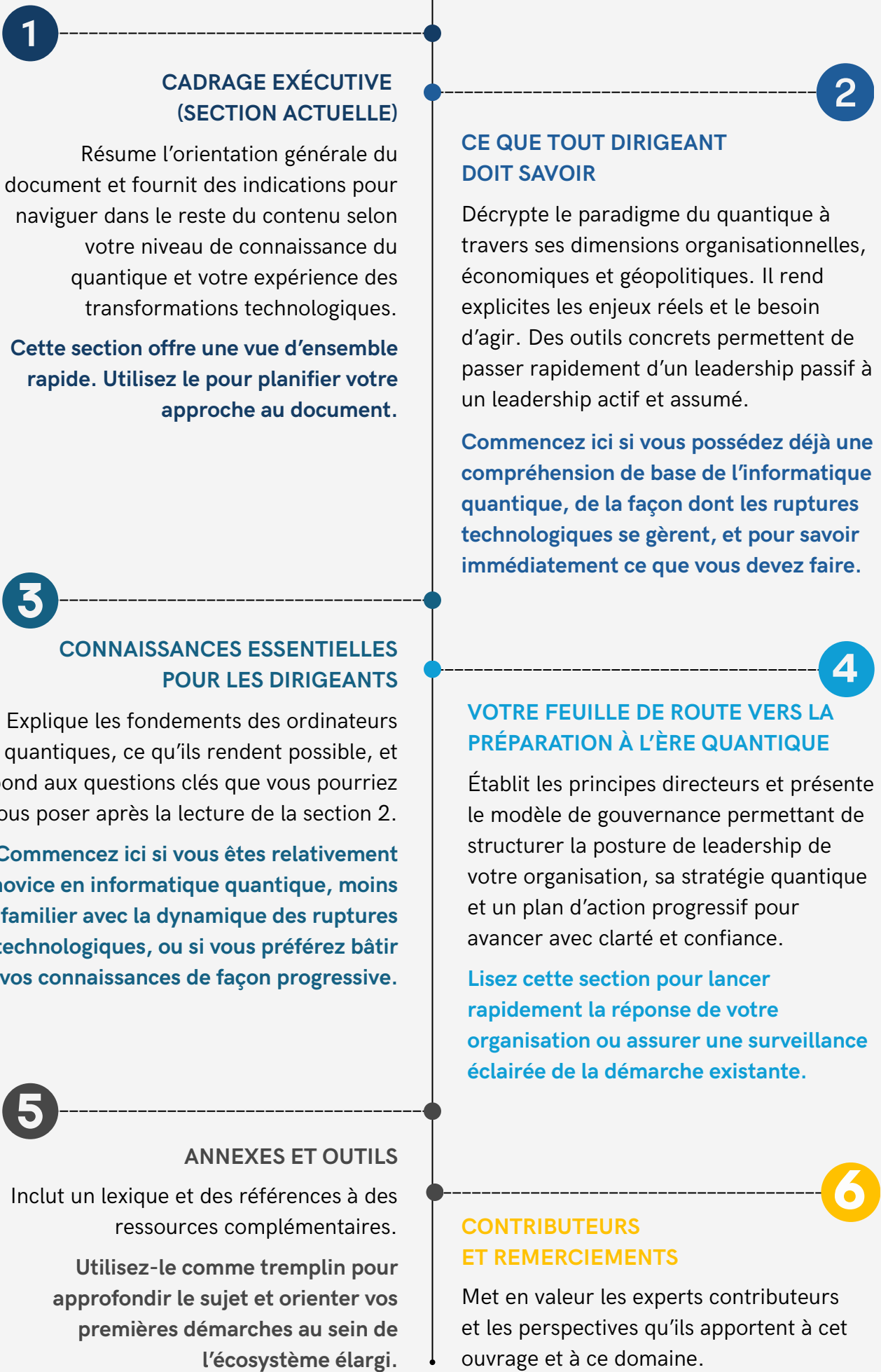
À qui s'adresse-t-il ?

Administrateurs de conseil
et dirigeants exécutifs

Les administrateurs et les dirigeants exécutifs ayant la responsabilité fiduciaire de protéger leur organisation et la confiance du public constituent le public principal de ce guide.

Grandes institutions
financières et publiques

Bien que pertinent pour toutes les organisations, ce guide cible surtout les grandes institutions financières et publiques, où les enjeux et l'impact sur la sécurité nationale, l'économie et la souveraineté technologique sont les plus élevés.



Les repères essentiels pour diriger



Les gagnants seront ceux qui apprendront et agiront plus vite que l'évolution du paysage.

Cette section du guide pose le cadre des enjeux et des raisons d'agir. Les sections suivantes en proposent une analyse plus détaillée.

L'élan est indéniable : la question clé n'est plus de savoir si les ordinateurs quantiques deviendront un moteur de transformation, mais quand.

Les percées en ingénierie quantique s'accroissent ; les gouvernements redoublent d'efforts et d'investissements, tandis que les agences de sécurité nationale se mobilisent pour protéger les données sensibles en prévision du « Q-Day ». Parallèlement, des leaders des secteurs de la finance, de la pharmacie, de l'énergie et de la logistique expérimentent des cas d'usage, bâtissent des feuilles de route et sécurisent expertises et partenariats clés. Pourtant, malgré cette dynamique, la majorité des organisations ne sont ni prêtes ni outillées pour en anticiper les impacts. Souvent, le sujet n'est même pas à leur radar. Lorsqu'elles relèveront la tête, le quantique aura déjà redessiné le terrain, sur les plans numérique, économique et géopolitique.

Les capacités du calcul quantique portent à la fois promesse et menace. Elles accéléreront les avancées scientifiques, aideront à résoudre des défis industriels complexes et pourraient alléger la pression de l'IA sur les systèmes énergétiques. À l'inverse, elles permettront d'exposer des données sensibles et menaceront la stabilité des communications, des économies et de la sécurité nationale, en fragilisant la confiance numérique.

Le **Q-Day** marque le moment où les ordinateurs quantiques deviendront assez puissants pour briser de nombreuses méthodes actuelles de chiffrement et d'authentification, exposant des informations protégées et sapant les fondements de la confiance numérique. Cela tient au fait que leurs bases mathématiques reposent sur des problèmes que les ordinateurs quantiques savent résoudre efficacement. De façon critique, même si le **Q-Day** est à venir, **le risque est déjà réel** : des données sensibles sont dès aujourd'hui collectées pour être déchiffrées et exploitées plus tard.



Pourquoi cette fois-ci est-elle différente ?

Comme tout outil, les ordinateurs quantiques sont intrinsèquement neutres : ils reflètent les intentions de ceux qui les utilisent. Qu'ils servent à relever les plus grands défis de l'humanité ou à accentuer les inégalités dépend entièrement des choix que nous faisons, comme dirigeants, innovateurs et citoyens. Ce qui change cette fois-ci, c'est **l'ampleur des risques** et la réalité troublante que le contrôle de cet outil, et de ses usages, nous échappe largement.

Sur le terrain, l'impératif est clair : **une mobilisation immédiate est requise**. À l'inverse, pour ceux qui portent une responsabilité fiduciaire, le débat demeure souvent opaque, enfermé dans un jargon technique trop abstrait pour guider l'action.

Pendant ce temps, la puissance du calcul quantique s'accroît, le Q-Day se rapproche et les risques s'intensifient pour ceux qui ne se préparent pas. Ce n'est qu'en rendant ces impératifs explicites pour les conseils d'administration et les dirigeants que le leadership peut réellement s'exercer. **Décomposons-les.**

2.1

Ce que tout dirigeant doit savoir

Ce qui peut sembler une percée soudaine est en réalité le fruit de décennies de recherche rigoureuse et de vision stratégique. Cette même clairvoyance rend une chose évidente : ***les enjeux n'ont jamais été aussi élevés.***

Voici les principales considérations d'un avenir quantique :

Cybersécurité

Les ordinateurs quantiques tolérants aux fautes remettront en cause de nombreuses méthodes actuelles de chiffrement et d'authentification, mettant en péril les données et canaux de communication qui en dépendent. L'impact sera universel, touchant pays, organisations et individus connectés à Internet. La menace dépasse la confidentialité : elle atteint l'intégrité même des identités numériques. Une compromission à ce niveau pourrait **provoquer un effondrement systémique de la confiance numérique** - ce socle invisible qui rend possibles le commerce, la coordination et la prise de décision à l'échelle mondiale.

Avantage stratégique

Les ordinateurs quantiques permettront de résoudre des problèmes hors de portée des systèmes classiques, créant des avantages stratégiques décisifs pour les pays et les organisations capables d'en tirer parti. Ces avantages s'étendront à des secteurs clés comme la finance, la santé, l'énergie et la logistique. Les acteurs précoces sécurisent déjà partenariats, propriété intellectuelle et talents, se positionnant pour longtemps. Contrairement à l'IA, qui s'est appuyée sur des infrastructures existantes facilement extensibles, le quantique ne dispose d'aucune base comparable. **Les retardataires risquent d'en être durablement exclus, sans véritable possibilité de rattrapage.**

Écart de capacités

Préparer un pays ou une grande organisation à faire face à ces risques et à saisir ces opportunités exige des années de travail en amont. De nouvelles expertises et capacités sont nécessaires, soutenues par des fonctions, politiques, processus, ainsi que par de nouveaux outils et technologies. Or, bâtir ces capacités prend du temps. De la même façon que peu d'organisations ont su déployer des solutions d'IA fiables et sécurisées trois ans après son émergence, **attendre que le « quantique soit prêt » garantit que vous ne le serez pas.**

Souveraineté

En raison de son potentiel exceptionnel, à la fois comme menace et comme avantage stratégique, le calcul quantique est appelé à remodeler les dynamiques économiques et politiques mondiales. Le développement d'expertises, d'industries et d'écosystèmes quantiques nationaux afin de renforcer la **souveraineté numérique et technologique est devenu essentiel** dans un contexte d'incertitude politique et de tensions persistantes sur le tissu social mondial.

Le carrefour quantique du Canada

Grâce à une génération de visionnaires, **le Canada occupe une position de leadership rare** dans le paysage quantique mondial. Il affiche l'un des plus hauts ratios par habitant de scientifiques, d'ingénieurs et d'entreprises quantiques. Mais nous avons déjà vécu ce moment, et l'histoire nous a livré une leçon claire⁹. Préserver cet avantage exige plus que l'excellence académique et l'esprit entrepreneurial. Cela requiert des efforts coordonnés pour soutenir des écosystèmes d'innovation industrielle, avec **l'engagement actif des grandes organisations**, banques, manufacturiers, services publics et gouvernements, afin de transformer notre force scientifique en puissance économique durable et en influence politique.

Rôle de la finance

La finance est idéalement positionnée, et en partie responsable, de se mobiliser et d'entraîner les autres secteurs, car elle est la **gardienne de l'infrastructure mondiale de confiance**. Un risque quantique non maîtrisé menace cette confiance numérique, fondement des transactions et de la confiance des marchés. Plus que tout autre secteur, **la finance peut et doit piloter la préparation quantique mondiale** en s'appuyant sur son expertise interne, ses structures internationales et son influence¹⁰ sur les réseaux de confiance pour fixer des standards et coordonner la migration cryptographique post-quantique à l'échelle transfrontalière.

2.2

Votre appel à l'action

Une action immédiate s'impose, non seulement en raison de l'ampleur des enjeux, mais aussi parce que la fenêtre de préparation se referme.

Voici les principales considérations d'un avenir propulsé par le quantique :

- 1 Il ne s'agit pas d'un risque futur, mais d'une menace actuelle.**
Des acteurs malveillants peuvent déjà capter des données chiffrées et des certificats numériques afin de les exploiter ultérieurement, lorsque la pleine puissance quantique sera disponible. Les menaces « *Harvest Now, Decrypt Later* » et « *Trust Now, Forge Later* » **exposent toute information dont la durée de vie dépasse quelques années**, y compris les données historiques et patrimoniales.
- 2 Votre responsabilité fiduciaire peut déjà être engagée.**
Les lois sur la protection de la vie privée et des données obligent les organisations à mettre en place des mesures de sécurité appropriées, certaines engageant directement la responsabilité des administrateurs en cas d'omission. Or, ces exigences évoluent et de nombreux organismes de normalisation ont clairement signalé l'intensification des risques en cybersécurité liés au quantique.¹¹ **L'inaction pourrait bientôt être interprétée comme un choix.**
- 3 Cette fois, les conséquences seront différentes.**
Un choc brutal est différent d'une érosion progressive. Jusqu'à présent, l'impréparation face à l'IA s'est traduite par des pertes de compétitivité et d'efficacité. L'impréparation quantique, elle, fait peser un **risque de rupture nette**, pouvant entraîner des années de gestion de crise et de remédiation en cybersécurité. De même, les organisations qui n'auront pas développé leurs capacités internes peineront à attirer les talents, les ressources et les partenaires nécessaires pour **rester compétitives** face aux opportunités quantiques.

⁹ Le Canada a fait preuve d'un leadership précoce en aérospatiale, en télécommunications et en IA, qu'il n'a pas su soutenir dans le temps.

¹⁰ Le *Financial Services Information Sharing and Analytic Services Center* (FS-ISAC) collabore déjà avec de nombreuses institutions à l'échelle internationale; il est maintenant temps de nous organiser et de démontrer un leadership collectif au niveau national.

¹¹ Par exemple, le *National Institute of Standards and Technology* (NIST) et le Centre canadien pour la cybersécurité (CCCS) fournissent des orientations claires.

4 Notre avantage concurrentiel national est en jeu.

Sans mobilisation à grande échelle, les innovations canadiennes seront monétisées ailleurs, tout en fragilisant la résilience nationale, la souveraineté technologique et, avec elles, l'accès de votre organisation aux compétences critiques, aux plateformes sécurisées et aux chaînes d'approvisionnement fiables des prochaines années. Innover sans commercialiser ne mène nulle part. Nous avons démontré notre capacité à diriger, mais aussi une tendance à laisser filer notre avance. **Ne répétons pas cette erreur avec le quantique.**

5 Les organisations ont besoin de temps pour se mobiliser.

La préparation d'une entreprise à une rupture technologique majeure exige un leadership décisif et s'étend, en moyenne, sur **plus de trois ans**. Les dirigeants doivent être formés et alignés, les stratégies ajustées, les budgets réalloués, les équipes formées, les modes de décision adaptés et des capacités durables mises en place. Rien de cela ne se fait du jour au lendemain, sans même compter la migration elle-même, qui prendra beaucoup plus de temps.

6 Des efforts et une complexité majeurs nous attendent.

La migration de votre infrastructure cryptographique est un chantier d'envergure. Pour les grandes organisations, il pourrait s'agir de **la migration technologique la plus complexe jamais entreprise**¹². C'est un processus d'exploration, riche en inconnues, qui touche à la racine de vos infrastructures et au cœur de votre chaîne de confiance. De multiples décisions devront être prises pour évaluer les impacts de chaque changement¹³. L'ampleur et l'effort requis seront considérables, en particulier pour les institutions financières.

7 Nous disposons des outils pour nous protéger.

Les normes de cryptographie post-quantique¹⁴ et les technologies pour les mettre en œuvre **existent déjà**. Mieux encore, une expertise de calibre mondial et des produits de pointe sont développés ici même, au Canada. S'appuyer sur des systèmes cryptographiques conçus par des entreprises canadiennes renforce notre souveraineté numérique et technologique.

8 Notre écosystème quantique a besoin de vous.

Nos universités et nos industries quantiques regorgent de talents et développent les solutions nécessaires pour permettre à votre organisation de tirer parti du potentiel du quantique. Mais l'innovation ne peut progresser en vase clos. Les problèmes concrets stimulent l'innovation réelle. Nous avons atteint un stade où les partenariats sont essentiels et **généreront des bénéfices partagés** pour l'écosystème et pour les organisations qui s'y engagent.

9 Surmonter les barrières traditionnelles.

La **collaboration et la transparence** entre des acteurs historiquement protecteurs seront déterminantes pour assurer la souveraineté nationale et créer de la valeur collective. Face à l'ampleur des besoins de l'ère quantique, une approche cloisonnée, fondée sur la rétention d'informations stratégiques et d'avantages techniques, empêchera l'écosystème national de franchir le cap vers la souveraineté quantique.

10 Il existe une feuille de route.

Ce guide vous apporte les **connaissances essentielles et la clarté nécessaires pour agir**, avec une approche structurée, étape par étape, afin de naviguer entre opportunités et menaces quantiques : posture de risque imminent (0-12 mois), expérimentation et développement des capacités d'entreprise (0-2 ans), et création d'avantages stratégiques (3 ans et plus).

¹² Voir *Quantum Readiness / PQC Migration Is the Largest, Most Complex IT/OT Overhaul Ever*, par Marin Ivezic, pour mesurer l'ampleur du chantier.

¹³ Voir l'annexe pour les meilleures pratiques et le guide du CFDIR-QEWG, qui clarifient l'ampleur des travaux de migration post-quantum.

¹⁴ La cryptographie post-quantique (PQC) est conçue pour résister aux attaques des ordinateurs quantiques et assurer la sécurité continue des communications numériques et des données à l'ère quantique.

2.2.1

Boussole d'urgence

Cette boussole d'urgence montre comment la vitesse de mobilisation et l'ampleur de votre réponse détermineront si votre organisation mènera ou subira le choc du Q-Day. Utilisez-la conjointement avec le **théorème de Mosca**¹⁵ pour structurer les discussions sur votre vision organisationnelle et communiquer des attentes claires à vos équipes de préparation quantique.



Axes expliqués

Axe horizontal – Vitesse de mobilisation

Représente le temps nécessaire à votre organisation pour définir et exécuter sa stratégie quantique. Plus **vous tardez à agir et à livrer**, plus il devient difficile de sécuriser les compétences et ressources requises et de maîtriser les risques. Les précurseurs bâtissent leurs capacités de façon intentionnelle; **les retardataires subissent des réactions coûteuses**.

Axe vertical – Rapidité d'arrivée du Q-Day

Représente le délai avant que la disruption quantique ne devienne concrète. Le bas de l'axe indique un Q-Day précoce, le haut un Q-Day plus tardif. **Une arrivée soudaine ou anticipée du Q-Day** laissera les retardataires, ou ceux sans plan de migration efficace, **désorganisés ou à l'arrêt**.

¹⁵ Selon le théorème de Mosca, les données à longue durée de vie sont déjà à risque si la durée de protection requise plus le temps de migration excèdent l'horizon d'arrivée des ordinateurs quantiques puissants.



2.3

Ce guide est conçu pour aider les administrateurs et dirigeants à approfondir leur compréhension des actions à mener de façon stratégique et responsable.

Ce que vous devez savoir

En tant que dirigeant assumant des responsabilités fiduciaires, voici ce que vous devez savoir :

- Les impacts de cette nouvelle classe technologique sur votre organisation et ses effets potentiels à l'échelle mondiale, tant en matière de risques que d'opportunités.
- L'évolution du paysage quantique et la façon dont elle transforme les menaces et opportunités auxquelles votre organisation est confrontée.
- Votre rôle et vos responsabilités pour guider votre organisation face à une disruption technologique de cette ampleur.
- Qui est responsable de vous tenir informé et de piloter la réponse de votre organisation, et si cette fonction dispose des ressources nécessaires pour agir efficacement.

Agir proactivement coûte moins et crée de la valeur¹⁶, alors qu'une crise prolongée laisse des séquelles durables à l'organisation.

2.4

Prochaines étapes immédiates pour les dirigeants

En tant que membre d'un conseil ou d'une équipe de direction, vous devez faire preuve de clairvoyance et d'urgence face aux risques et opportunités du quantique.

Cette section propose une **vue pragmatique et de haut niveau** du travail à venir. Utilisez-la comme guide rapide pour exercer une gouvernance responsable et positionner votre organisation afin de créer de l'avantage à mesure que l'ère quantique se déploie. La section 4, Votre feuille de route vers la préparation à l'ère quantique, **détaille l'ampleur des travaux** requis pour une stratégie de préparation complète et efficace.

La première année sera exigeante. Rappelez-vous toutefois que plus vous agissez tôt et vous préparez bien, plus vous réduisez les risques et les coûts futurs.

Voici ce que vous devez faire :

Prochains
0 à 90
jours

Assumer votre responsabilité fiduciaire

N'attendez pas la réglementation.

Elle arrive, les signaux sont clairs. Attendre ne fait que vous placer en désavantage stratégique tout en augmentant vos risques et vos coûts.

Bâissez votre compréhension stratégique¹⁷.

Déployez un programme de formation pour le conseil et la haute direction afin de bien comprendre les implications de cette nouvelle classe de technologies. Exigez ensuite des formations et des séances d'information continues pour rester à jour et suivre l'évolution du paysage.

Sécurisez les expertises clés.

Vous avez besoin de talents couvrant plusieurs domaines¹⁸ pour guider votre organisation de façon sécuritaire et stratégique. Personne n'a encore fait ce parcours, mais certains s'y préparent depuis longtemps¹⁹. Entourez-vous de ces experts.

Mandatez une stratégie de défense post-quantique.

Demandez à la direction de lancer un programme quantique sécurisé pour moderniser l'infrastructure cryptographique de l'organisation. Comme premier livrable, exigez un plan clair définissant la démarche d'élaboration du plan.

¹⁶ Au-delà des gains internes, une préparation précoce accroît la confiance des investisseurs, qui intègrent désormais la gestion des risques technologiques et la préparation quantique à leurs critères de gouvernance et de valorisation.

¹⁷ Consultez ldiq.ca pour découvrir les programmes de formation de LDIQ à l'intention des conseils et des dirigeants.

¹⁸ Formateurs en quantique, experts en post-quantum encryption, modélisateurs issus de la physique, décideurs et gestionnaires de risques sensibilisés au quantique.

¹⁹ Le *Quantum-Readiness Working Group* (QRWG) du Forum canadien pour la résilience des infrastructures numériques (FCRIN) constitue un excellent exemple de pionniers et experts canadiens dans ce domaine.

Prochains
90 à 180
jours

S'organiser pour réussir

Établissez une « équipe de préparation quantique ».

La préparation au quantique couvre de multiples dimensions et requiert des expertises variées. Mettez en place une équipe de leadership multidisciplinaire pour regrouper les compétences, coordonner la réponse et éviter une approche fragmentée ou en silos.

Commanditez une évaluation de haut niveau des risques et opportunités.

L'objectif est d'obtenir une première vision de ce qui est en jeu pour votre organisation, au-delà de l'urgence cryptographique, et d'ouvrir le champ des possibles en matière d'opportunités.

Mettez en place une gouvernance et un reporting formels.

Identifiez les décisions clés et les responsabilités, et instaurez un reporting trimestriel sur la préparation, les risques et les enjeux réglementaires afin d'assurer l'imputabilité et la vision à long terme. Définissez votre position sur la souveraineté numérique et technologique ainsi que le rôle de votre organisation dans l'écosystème national.

Alignez-vous sur votre posture défensive.

Déterminez le quadrant visé de la boussole d'urgence et votre estimation interne du Q-Day. Ancrez un discours clair sur les implications pour votre appétence au risque, vos priorités stratégiques et vos communications à vos employés et avec les parties prenantes.

Connectez-vous à vos pairs du secteur.

Les enjeux sont majeurs. Sur les questions de confiance numérique et de souveraineté, la collaboration crée plus de valeur que l'isolement. Appuyez-vous sur les forums sectoriels et les échanges entre pairs pour partager les plans de migration post-quantique.

Prochains
180 à 270
jours

Élargissez le champ

Publiez votre feuille de route défensive.

Elle doit inclure, en priorité, un volet de développement de la cryptoagilité ainsi qu'un volet de migration vers la cryptographie post-quantique, en précisant les hypothèses de base, les ressources requises et les échéanciers estimés.

Allouez des investissements à long terme.

Traitez le chiffrement post-quantique comme un investissement pluriannuel, pas un projet ponctuel. Allouez des budgets pour l'inventaire, la migration, la formation, les fournisseurs et les tests en continu.

Identifiez vos opportunités de cas d'usage quantiques.

Utilisez-le ou perdez-le. Bâissez un pipeline de cas d'usage quantiques à valeur ajoutée. Centralisez vos analystes et modélisateurs familiers du quantique et développez votre expertise interne.

Engagez des guides et des partenaires clés.

Si ce n'est pas déjà fait, établissez dès maintenant des partenariats avec les acteurs du quantique. La demande va s'accélérer à l'approche du Q-Day. Agissez tôt pour sécuriser votre place dans la chaîne d'approvisionnement nationale et la capacité de vos partenaires à vous soutenir.

Prochains
270 à 360
jours

Mettez à profit votre position de leadership.

Renforcez vos politiques et la conformité.

Revoyez les politiques clés, dont l'approvisionnement, la sécurité et les risques tiers. Imposer des contrôles pour forcer le respect des standards post-quantiques et exiger des feuilles de route et une posture de souveraineté dans les contrats et appels d'offres.

Engagez-vous dans l'écosystème des normes.

Participez aux forums nationaux et internationaux pour façonner les normes et protocoles, influencer les calendriers d'adoption et renforcer la position de votre organisation et celle du pays.

2.3

Questions clés à poser par les dirigeants

Voici une liste de questions que les dirigeants et les membres du conseil devraient poser afin d'établir la posture de leur organisation en matière de préparation au quantique.



- Cette rupture technologique est-elle suffisamment majeure pour justifier une supervision au niveau du conseil ? (Oui)
- Les membres du conseil et de la direction maîtrisent-ils suffisamment les enjeux liés au quantique ?
- Quelle est notre exposition actuelle ? Quelles données à longue durée de vie détenons-nous et quelle est notre estimation du Q-Day ?
- Où les technologies quantiques peuvent-elles créer de nouvelles opportunités ou un avantage concurrentiel pour notre organisation ?
- Quelle est notre ambition quantique (précurseur, suiveur, observateur prudentier) ?
- Dans quel quadrant de la boussole d'urgence voulons-nous nous situer au Q-Day ?
- Avons-nous recensé tous nos systèmes cryptographiques, données et canaux de communication, et identifié ceux qui sont vulnérables ?
- Disposons-nous d'une feuille de route vers une cryptographie sécurisée face au quantique, avec des ressources et des priorités suffisantes ?
- Avons-nous un plan si le quantique arrive à maturité avant que nous soyons prêts ?
- Quelle est notre position sur la souveraineté numérique et technologique, notamment en matière de quantique ?
- Quel rôle jouons-nous dans la gouvernance de l'écosystème quantique ?
- Quels mécanismes avons-nous pour suivre normes, réglementations et menaces émergentes en quantique et en cryptographie ?
- Quelles implications juridiques ou fiduciaires pourraient émerger à mesure que le quantique redéfinit les attentes de surveillance ?
- Qui, au sein de la direction, pilote la préparation quantique ?
- Avons-nous les expertises nécessaires pour définir et exécuter notre réponse ?

Consultez l'annexe pour d'autres questions à poser une fois votre posture initiale établie.

Connaissances additionnelles pour les dirigeants

“

Le savoir confère du pouvoir, mais c'est la compréhension qui permet de l'utiliser avec assurance.

Cette section enrichit le contexte et les détails. Servez-vous-en pour renforcer vos connaissances et affiner votre compréhension.

3.1

Qu'est-ce que l'informatique quantique ?

3.1.1



Q : Ordinateurs quantiques vs classiques : quelles différences ?

La différence fondamentale entre ordinateurs quantiques et classiques réside dans leur architecture et leur façon de représenter l'information.

Les ordinateurs classiques utilisent des bits, qui prennent une valeur définie, 0 ou 1. Les ordinateurs quantiques reposent sur des qubits, capables d'exister simultanément dans plusieurs états grâce aux principes de la mécanique quantique. Cette propriété leur confère un avantage pour certains problèmes précis, comme la simulation moléculaire, la remise en cause de méthodes cryptographiques ou l'optimisation de systèmes complexes. Pour ces usages, ils peuvent surpasser largement les ordinateurs classiques.

Il est essentiel de comprendre qu'ils ne sont pas simplement plus rapides : **ce sont des outils fondamentalement différents**, adaptés à des tâches spécifiques.

3.1.2



Q : Faut-il maîtriser la physique quantique pour comprendre le sujet ?

Non. La physique quantique est profondément contre-intuitive et difficile à maîtriser. En tant que dirigeant ou administrateur, vous n'avez pas besoin d'en comprendre les fondements ni les détails techniques du calcul quantique au-delà de ce qui est présenté dans ce guide.

Concentrez-vous sur la stratégie, sur la mise en place de la bonne équipe et sur les moyens nécessaires à son efficacité, incluant connaissances, ressources et budgets.

3.1.3



Q : Quelles industries tireront parti du calcul quantique ?

Tout secteur confronté à la complexité, à l'incertitude ou à l'optimisation peut bénéficier du calcul quantique. Sa capacité à traiter des problèmes multidimensionnels et à simuler la réalité à l'échelle quantique transformera en profondeur la façon dont ces industries conçoivent, prédisent et prennent des décisions.



Pharmaceutique et santé

Le calcul quantique pourrait transformer la découverte pharmaceutique et la recherche biomédicale grâce à la simulation précise des molécules et protéines, accélérant l'identification des composés et écourtant coûts et délais des essais cliniques.

Énergie et matériaux

Les entreprises de l'énergie pourraient exploiter la modélisation quantique pour concevoir de nouveaux catalyseurs, matériaux supraconducteurs et batteries plus efficaces, ouvrant la voie à des avancées en stockage d'énergie, hydrogène et captation du carbone. L'optimisation quantique permettrait aussi d'améliorer en temps réel la gestion des réseaux électriques.

Transport et logistique

Les compagnies aériennes, maritimes et les acteurs de la logistique font face à des problèmes complexes de planification et de routage. L'optimisation quantique pourrait réduire les retards, la consommation de carburant et les émissions, tout en améliorant la résilience des flottes, des itinéraires et des réseaux de chaînes d'approvisionnement.

Manufacturier et aérospatiale

La simulation quantique des matériaux au niveau atomique ouvre la voie à des matériaux plus légers et robustes, des procédés optimisés et une production plus durable. Elle pourrait aussi améliorer la modélisation des turbulences et de l'aérodynamique, renforçant la conception des ailes, moteurs et surfaces de contrôle.

Sciences du climat et de l'environnement

Les simulations quantiques peuvent améliorer les prévisions météorologiques, la modélisation du climat et la recherche sur la capture du carbone, permettant aux gouvernements et aux entreprises de prendre des décisions d'adaptation et d'atténuation mieux éclairées.

Services financiers

En dernier lieu, le secteur financier est l'un des plus avancés pour bénéficier du quantique et l'adopter, grâce à ses capacités internes et à ses besoins critiques en optimisation et en gestion du risque. Parmi les cas d'usage clés :

- **Optimisation de portefeuille** : analyse simultanée de milliers d'actifs et de contraintes pour maximiser le rendement sous contrainte de risque.
- **Risque de crédit et de marché** : simulations quantiques capables de modéliser des dépendances complexes et des risques extrêmes, au-delà des approches Monte Carlo traditionnelles.
- **Fraude et anomalies** : détection plus rapide et plus fine de comportements atypiques dans des volumes transactionnels très élevés.
- **Liquidité et collatéral intrajournaliers** : optimisation en temps réel des flux et des sûretés entre devises et juridictions afin de réduire coûts et risques.
- **Exécution des transactions** : amélioration des stratégies algorithmiques pour limiter slippage, latence et frais.
- **Risques climatiques et ESG** : intégration conjointe des modèles climatiques et des expositions financières pour une évaluation plus fidèle des risques de long terme.

Ces exemples, aussi impressionnants soient-ils, ne marquent que le commencement. Avec la maturation du quantique et la diffusion des compétences dans les industries, des applications inédites et inattendues apparaîtront, rappelant l'impact des premières vagues d'analytique avancée et d'IA.

3.1.4 ? Q : Les ordinateurs quantiques remplaceront-ils les classiques ?

Non. Les avantages des ordinateurs quantiques se limitent à certains types de problèmes. Ils ne remplacent donc pas l'informatique classique, mais agissent comme des outils spécialisés offrant des gains décisifs pour des cas précis. Les superordinateurs classiques continueront d'évoluer et d'opérer aux côtés du quantique, chacun exploitant ses forces propres.

3.1.5 ? Q : Quels sont les risques liés à l'informatique quantique ?

Le principal risque tient au potentiel des ordinateurs quantiques tolérants aux fautes de **bouleverser la cybersécurité mondiale**.

Sans mesures d'atténuation, ce risque transformera en profondeur l'ensemble de nos vies, du numérique au physique. Il se décline en plusieurs niveaux. **Examinons-les, un à un.**



Première couche : atteinte à la confidentialité

C'est le risque le plus souvent cité. La capacité des ordinateurs quantiques à briser les protections cryptographiques existantes entraînera la divulgation de données confidentielles, qu'il s'agisse d'identités personnelles, de secrets industriels ou d'informations militaires critiques.



« Harvest Now, Decrypt later »

En lien direct avec la première couche, la menace *Harvest Now, Decrypt Later* (« collecter maintenant, déchiffrer plus tard ») est déjà active. Des acteurs malveillants collectent déjà des données chiffrées dans l'intention de les exposer ultérieurement à l'aide de futurs ordinateurs quantiques. Elle impose une action immédiate. Toutes les données dont la sensibilité s'étend sur plusieurs années sont concernées.



« Trust Now, Forge Later »

Trust Now, Forge Later (« faire confiance maintenant, falsifier plus tard ») constitue le prolongement dynamique de « Harvest Now, Decrypt later ». Alors que ce dernier expose des données confidentielles, le premier s'attaque aux certificats, aux signatures numériques et aux processus d'authentification. Des identités forgées permettent des intrusions silencieuses, sous une apparence légitime, avec les mêmes droits que des utilisateurs de confiance.

Cette menace sur l'identité numérique dépasse celle liée à la confidentialité, puisqu'elle sape **la nature même de la confiance numérique**.

Pourquoi la confiance numérique est-elle un enjeu critique ?

La confiance numérique est le fondement invisible qui rend possibles des transactions fiables, des communications sécurisées et le fonctionnement du quotidien numérique. Elle soutient Internet et tous les systèmes connectés sur lesquels repose la société moderne, des environnements commerciaux aux usages publics et personnels.

Comme une pièce d'identité et une signature dans le monde physique, les certificats et signatures numériques authentifient nos actions en ligne et celles des systèmes informatiques.

La falsification de certificats ou de signatures numériques offrirait à des acteurs malveillants un accès furtif aux réseaux sous des identités usurpées, leur permettant de contester la propriété de l'information et d'intervenir sur des systèmes industriels, des infrastructures critiques, la santé, le transport et la défense. Dans ces contextes, une atteinte à l'intégrité est plus grave qu'une atteinte à la confidentialité.

Des capacités de falsification numérique permises par le quantique pourraient interrompre des services essentiels, fragiliser des chaînes d'approvisionnement entières et entraîner des conséquences physiques en cascade. Si le risque lié à *Harvest Now, Decrypt Later* est bien compris, c'est la **menace sur l'identité numérique qui représente le risque le plus élevé**.

Dès que vous comprenez la menace qui pèse sur la confiance numérique²⁰, l'urgence d'agir immédiatement s'impose.

Synthèse des risques

Une vision élargie des risques comprend²¹ :

1

Risque de perte de confiance à l'échelle de l'économie numérique (*Trust Now, Forge Later*)

3

Risque de perte de souveraineté sur des technologies ou services critiques

2

Risque d'exposition de données confidentielles (*Harvest Now, Decrypt Later*)

4

Risque de perte d'opportunités et d'avantage quantique au profit des concurrents

3.1.6



Q : Qu'est-ce que la cryptographie post-quantique ?

Commençons par la cryptographie dans son ensemble. Elle constitue le système qui protège l'information en assurant que les données, messages, commandes et transactions ne sont accessibles ou exécutables que par des parties autorisées et vérifiables. Elle s'appuie sur plusieurs mécanismes clés, dont le chiffrement, les signatures numériques, les certificats d'authentification et les protocoles sécurisés d'échange de clés.

Au cœur de ce dispositif se trouve l'infrastructure à clé publique (*Public Key Infrastructure*), qui permet de créer, gérer, distribuer, utiliser et révoquer des certificats numériques et des clés cryptographiques à l'échelle mondiale. Ces clés sont le fondement des fonctions numériques sécurisées, telles que le chiffrement, les signatures numériques et l'authentification.

Les systèmes cryptographiques s'appuient sur des algorithmes mathématiques. Leur sécurité repose sur le fait que ces algorithmes soient impossibles à briser dans un délai raisonnable avec les technologies actuelles et anticipées. Depuis trois décennies, la plupart des algorithmes cryptographiques reposent sur des problèmes mathématiques que les ordinateurs classiques ne pouvaient résoudre de manière praticable. L'émergence d'ordinateurs quantiques suffisamment puissants changera cette réalité.

La cryptographie post-quantique constitue la nouvelle génération d'algorithmes cryptographiques. Elle repose sur des problèmes mathématiques pour lesquels aucun avantage quantique n'est connu aujourd'hui et dont les experts jugent peu probable l'apparition. Elle ne requiert pas de technologie quantique et est conçue pour être déployée efficacement sur des environnements informatiques classiques.

Pour maintenir la confiance numérique à l'ère quantique, tous les systèmes numériques devront migrer vers des standards et des pratiques de cryptographie post-quantique.

Il ne s'agit pas d'une simple mise à jour logicielle. Penser que la migration post-quantique est un ajustement mineur ou un problème relevant uniquement des fournisseurs est une erreur répandue. Les systèmes cryptographiques sont profondément intégrés à l'architecture réseau. De légères modifications des échanges cryptographiques peuvent produire des répercussions inattendues à l'échelle de l'infrastructure. Assurez-vous que vos équipes sont en mesure de comprendre et de vous présenter une vision complète des besoins et du plan de migration post-quantique de votre organisation.

3.1.7



Q : Qu'est-ce que la cryptoagilité, concrètement ?

L'époque où un seul ensemble d'algorithmes pouvait protéger durablement le monde numérique est terminée. La puissance de l'informatique quantique et la sophistication croissante de l'IA rendent toute complaisance cryptographique impossible.

Plus qu'une migration unique vers la cryptographie post-quantique, il faut bâtir une capacité d'adaptation continue et dynamique de l'infrastructure cryptographique. Les mises à jour seront constantes, les adversaires évolueront, et de nouvelles vulnérabilités et normes apparaîtront. Notre capacité à suivre devra évoluer tout autant.

Selon le FS-ISAC²², la **cryptoagilité** est « la capacité d'une organisation à adapter rapidement et efficacement ses solutions ou algorithmes cryptographiques, y compris paramètres et clés, face aux avancées en cryptanalyse, aux menaces émergentes, aux progrès technologiques ou aux vulnérabilités ». Elle est aussi définie comme « un principe de conception permettant de déployer, mettre à jour, remplacer et adapter la cryptographie et les processus d'affaires associés sans changements architecturaux majeurs, avec une perturbation minimale des opérations et des délais de transition courts ».

L'agilité, c'est la capacité d'agir vite, de façon maîtrisée. Elle résulte de la conscience, de la flexibilité et de la robustesse.

En pratique, la cryptoagilité n'est pas un enjeu technologique, mais un enjeu de capacités et de modèle opérationnel. Elle exige des cadres permettant aux équipes cryptographiques une visibilité fine des actifs et des menaces (conscience), une réelle autonomie décisionnelle (flexibilité) et des canaux, règles et contrôles fondés sur le risque clairement établis (robustesse) pour gérer les mises à jour de façon agile.

Dorénavant, toutes les organisations devront garantir leur cryptoagilité. **Il est temps d'écouter vos équipes TI, cyber et cryptographiques.**

²² Le FS-ISAC (Financial Services Information Sharing and Analysis Center) est un consortium sectoriel dédié à la réduction du cyber-risque dans le système financier mondial. Il soutient les institutions financières et, par extension, leurs clients. Il regroupe plus de 5 000 organisations membres présentes dans 75 pays.

3.1.8 ? Q : Quelle est la relation entre l'informatique quantique et l'IA ?

Longtemps développées séparément, l'informatique quantique et l'IA convergent aujourd'hui de manière à se renforcer mutuellement. Cette relation quantique-IA se structure en trois catégories, chacune correspondant à un degré de maturité distinct.

1

AI for Quantum (réalité actuelle) : l'IA contribue déjà directement aux avancées quantiques, en soutenant la conception du matériel, l'optimisation de l'exploitation des systèmes et l'amélioration des approches de correction d'erreurs. L'apprentissage automatique est notamment utilisé pour concevoir et optimiser des circuits quantiques, analyser et réduire le bruit matériel, et permettre une correction d'erreurs quantiques opérationnelle.

Statut et impact : c'est à ce jour l'axe le plus avancé et le plus impactant, avec des déploiements actifs en laboratoire et dans des outils industriels émergents. *AI for Quantum* améliore l'efficacité et la fiabilité des systèmes quantiques en conditions réelles.

2

Quantum-Inspired AI (le pont) : la *Quantum-Inspired AI* exploite des idées de la physique quantique pour rendre plus efficaces certaines tâches d'IA et d'optimisation sur les systèmes classiques d'aujourd'hui. Les réseaux de tenseurs, développés à l'origine pour la simulation de systèmes quantiques complexes, peuvent par exemple, compresser des modèles de grande taille et réduire les besoins en mémoire et en calcul, avec un impact limité sur la précision.

Statut et impact : ces approches sont déjà en usage, en particulier dans des outils commerciaux d'optimisation et de compression de modèles. Elles offrent un pont pragmatique et à court terme entre l'IA actuelle et les flux de travail futurs accélérés par le quantique.

La physique quantique à plusieurs corps s'intéresse aux systèmes où l'interaction de nombreuses particules quantiques fait émerger des comportements collectifs. Or, une grande partie des phénomènes au cœur des technologies quantiques modernes relève intrinsèquement de cette dynamique.

Les réseaux de tenseurs sont un cadre mathématique conçu pour représenter efficacement des systèmes complexes. Ils agissent comme une compression avancée des relations dans les données : au lieu de modéliser explicitement toutes les interactions possibles, qui explosent de manière exponentielle, ils décomposent le système en blocs élémentaires (tenseurs) interconnectés, capturant uniquement les dépendances essentielles.

3

Quantum for AI (potentiel futur) : à long terme, l'ambition est d'exécuter directement sur des processeurs quantiques certaines parties des flux de travail d'IA. Ce champ émergent, le *Quantum Machine Learning*, étudie dans quelle mesure les états et opérations quantiques peuvent accélérer ou améliorer des tâches d'apprentissage précises, et si des flux de travail bien structurés peuvent bénéficier de ressources quantiques.

Statut et impact : le *Quantum Machine Learning* en est encore à la recherche et au prototypage. Des avantages théoriques sont identifiés pour des cas d'usage très ciblés et, à terme, des processeurs quantiques évolutifs et tolérants aux fautes pourraient réduire la consommation d'énergie par calcul. En revanche, aucun avantage de performance en conditions réelles par rapport à l'IA classique de référence n'a encore été observé.

3.1.9



Q : Quelles capacités de calcul quantique sont disponibles aujourd'hui ?

À ce stade, des ordinateurs quantiques à faible fidélité et à échelle limitée sont déjà disponibles. Cette phase est désignée par l'industrie comme l'ère NISQ (*Noisy Intermediate-Scale Quantum*), le bruit faisant référence au taux d'erreur élevé qui caractérise ces systèmes.

Ces machines disposent d'un nombre restreint de qubits. Le défi majeur consiste à convertir ces qubits physiques bruités et instables en qubits logiques corrigés d'erreurs²³. L'augmentation du nombre de qubits logiques nous rapproche d'ordinateurs quantiques évolutifs et tolérants aux fautes, et des capacités qu'ils rendront possibles.

Dans la finance, la pharmacie et la logistique, des organisations pionnières utilisent déjà des ordinateurs quantiques bruités pour explorer leur potentiel applicatif. **Il est aujourd'hui simple de s'initier au quantique**, et ce choix est stratégiquement judicieux. Plusieurs fabricants offrent également des parcours d'expérimentation guidée et des preuves de concept packagées, avec des solutions adaptées aux besoins sectoriels.

Les partenariats établis dès maintenant avec l'écosystème du calcul quantique procureront un accès privilégié aux savoirs, aux talents et au matériel lorsque les ordinateurs quantiques tolérants aux fautes deviendront disponibles. À ce stade, la demande pour ces ressources rares sera intense.

3.1.10



Q : Quand les ordinateurs quantiques tolérants aux fautes arriveront-ils ?

Les estimations divergent : les investisseurs sont plus audacieux, certains universitaires plus réservés. Mais une chose ne fait aucun doute : la course est engagée.

Côté industrie, les feuilles de route de nombreux acteurs du quantique convergent vers un horizon de cinq ans, autour de 2030. Sur le plan défensif, le Centre canadien pour la cybersécurité impose aux organismes publics de sécuriser leurs systèmes critiques d'ici la fin de 2031. Dans cette perspective, **une évaluation prudente du risque situe l'arrivée possible du Q-Day vers 2030**, avec une probabilité qui augmente chaque année.

Il reste ainsi **moins de cinq ans** aux organisations pour bâtir les capacités requises et livrer les volets prioritaires de leur transformation. Même respecté, ce calendrier serré ne protège pas contre les menaces « *Harvest Now, Decrypt / Forge Later* », qui, pour plusieurs, pourraient déjà être une réalité.

3.1.11



Q : Quelle part relève du bruit médiatique et quelle part est réellement substantielle ?

Comme dans tout cycle technologique émergent, le bruit et la spéculation sont inévitables. Toutefois, des signaux clairs et indiscutables montrent que les technologies quantiques se rapprochent d'un niveau de préparation opérationnelle. Voici les signaux à observer :

- ✓ Investissements majeurs et engagements stratégiques d'acteurs industriels établis.
- ✓ Publications de politiques et de normes.
- ✓ Programmes et investissements publics.
- ✓ Transitions obligatoires avec échéances définies.
- ✓ Alignement des feuilles de route et engagements des grands fournisseurs.
- ✓ Résultats évalués par les pairs attestant de gains de performance mesurables.
- ✓ Projets pilotes sur des cas réels produisant des bénéfices quantifiés.
- ✓ Dynamique des consortiums sectoriels et playbooks.

Au T4 2025, tous ces signaux sont désormais clairement établis et vérifiables.

Il ne s'agit pas que de bruit.

²³ Certaines architectures de qubits peuvent nécessiter jusqu'à 1 000 qubits physiques pour créer un seul qubit logique.

3.1.12



Q : S'agit-il d'un nouveau moment Y2K ?

Oui, et Non.

Avant d'aller plus loin, recadrons le débat : si le Y2K a été un non-événement, c'est un résultat positif, pas un échec. Le risque a été neutralisé parce que des décisions ont été prises tôt, avec des responsabilités claires, des budgets et une coordination entre industries. La transition quantique exige aujourd'hui le même niveau de clairvoyance, d'action et de coordination pour être résiliente aux perturbations.

Dans cet esprit, comparons.

Oui, parce que

Un impact systémique mondial

Le Y2K a touché l'ensemble des systèmes, dans tous les secteurs, à l'échelle mondiale. Sa mitigation a exigé la mobilisation de tous les pays.

Une réponse portée par les organisations

Chaque organisation contribue à la réduction du risque et de l'impact systémiques en corrigeant ses propres plateformes et outils. Comme pour le Y2K, il faut penser globalement et agir localement.

Une synchronisation mondiale des standards

Bien que plus simple, le Y2K a nécessité un alignement sur des standards communs et la coordination de migrations complexes entre systèmes interconnectés.

Non, parce que

Une ampleur sans commune mesure

En 1999, Internet était encore embryonnaire et les technologies de l'information et opérationnelles étaient beaucoup moins répandues. Aujourd'hui, le nombre d'objets connectés a augmenté de plusieurs ordres de grandeur.

Une menace continue

Le Y2K comportait une échéance claire et une correction unique. Le Q-Day, lui, n'a pas de date connue et le risque est durable. L'évolution rapide et non bornée du quantique et de l'IA impose aux organisations de maintenir en permanence une avance grâce à la cryptoagilité.

Le risque est déjà présent

Même si ses effets ne sont pas encore perceptibles, les menaces *Harvest Now, Decrypt Later* et *Trust Now, Forge Later* impliquent que des données peuvent déjà être compromises. Une migration accélérée vers la cryptographie post-quantique réduit l'exposition, sans toutefois permettre d'annuler le risque comme ce fut le cas pour le Y2K.

Une action désormais plus stratégique

Le Y2K fut le premier test de gestion d'un risque technologique mondial, dans un contexte de maturité limitée des approches TI; certains travaux correctifs se sont révélés inutiles. Les pratiques actuelles, nettement plus avancées, permettent de cibler les risques prioritaires et de réduire plus efficacement les efforts non essentiels.

Témoignant de certaines similarités et de l'importance de ces deux événements, le terme « Y2Q » a fait une brève apparition en ligne en novembre 2025. Reste à voir s'il se généralisera.

3.1.13



Q : Quelle est l'étendue de mon devoir fiduciaire ?

En vertu de la Loi canadienne sur les sociétés par actions (LCSA), les administrateurs et dirigeants sont tenus à deux obligations principales : le devoir de diligence et le devoir de loyauté. Le devoir de diligence prévu par la LCSA exige que chaque administrateur et dirigeant, dans l'exercice de ses pouvoirs et l'exécution de ses fonctions, fasse preuve du soin, de la diligence et de la compétence qu'une personne raisonnablement prudente exercerait dans des circonstances comparables.

Le devoir de diligence impose aux administrateurs et dirigeants de mener des démarches suffisantes pour être pleinement informés et d'examiner toute information pertinente avant de prendre une décision. La LCSA prévoit aussi un devoir fiduciaire de loyauté, obligeant les administrateurs et dirigeants à agir honnêtement et de bonne foi dans l'intérêt supérieur de la société. Selon la Cour suprême du Canada, l'évaluation de cet intérêt peut intégrer, entre autres, les intérêts des actionnaires, des employés, des créanciers, des consommateurs, des gouvernements et de l'environnement.

La gestion et la surveillance des risques constituent une responsabilité centrale des conseils d'administration, incluant l'approbation d'un cadre d'appétit pour le risque et la supervision de sa mise en œuvre, de même que celle des contrôles internes associés. Par ailleurs, les lois en matière de protection des renseignements personnels imposent de plus en plus aux entreprises l'obligation de déployer des mesures de sécurité proportionnées à la sensibilité des données, couvrant l'ensemble de leur cycle de vie. Plusieurs régimes législatifs prévoient une responsabilité directe des administrateurs lorsqu'ils ont autorisé ou toléré un manquement.

La définition des mesures de sécurité jugées nécessaires évolue continuellement. Des organismes de référence, dont le NIST, signalent désormais des risques accrus en cybersécurité liés aux avancées de l'informatique quantique. Ces avancées créent donc des risques identifiés pour un grand nombre d'organisations. Il devient impératif que les administrateurs exercent dès maintenant une surveillance active de la façon dont la direction évalue les risques et les occasions associés au quantique pour l'entreprise.

3.1.14 ? Q : Quelles nouvelles capacités mon organisation doit-elle développer ?

Comme toute transformation majeure, l'organisation doit évoluer. Cela implique de développer de nouvelles capacités opérationnelles afin d'assurer non seulement la transition, mais aussi votre succès à long terme dans le nouveau paradigme quantique. Les axes clés à considérer incluent :

Gouvernance et risques  Les politiques doivent évoluer pour exiger la migration des fournisseurs vers des systèmes de cryptographie post-quantique, avec des mécanismes de contrôle assurant la conformité. Les rôles, les pouvoirs décisionnels et les considérations de souveraineté doivent être revus. De nouveaux indicateurs de risque doivent être mis en place.	Cybersécurité  De nouvelles capacités sont nécessaires pour surveiller et contrer une catégorie entièrement nouvelle de menaces. La cryptoagilité doit être développée afin d'assurer que votre organisation demeure alignée sur l'évolution des standards cryptographiques. Malgré un niveau d'effort déjà élevé, la cybersécurité doit gagner en cadence.	Partenariats stratégiques  Se préparer à l'ère quantique exige la construction d'un nouvel écosystème : partenariats stratégiques, nouveaux fournisseurs de confiance, engagement dans les standards, collaboration universitaire et mobilisation d'une communauté capable d'innover et d'agir ensemble.
Gestion des actifs  De nouvelles métadonnées doivent permettre de distinguer les données confidentielles durables des données à durée limitée. La gestion des actifs TI doit évoluer pour surveiller les vulnérabilités.	Processus et contrôles  Doivent évoluer pour intégrer les risques quantiques et respecter les nouvelles politiques et normes. Un pipeline dédié de cas d'usage quantiques doit structurer la sélection, l'évaluation et le financement des opportunités.	Expertise et effectifs  L'ère quantique exige de nouvelles compétences : algorithmes quantiques, gestion de la cryptographie, littératie quantique et gestion des risques actualisées, ainsi que la capacité de mener une migration à haute vitesse.

3.1.15



Q : Quel sera l'impact sur l'environnement ?

Les perspectives sont favorables. À maturité, les ordinateurs quantiques pourraient consommer moins d'énergie que les systèmes classiques pour les usages où ils excellent²⁴, devenant ainsi un levier clé de maîtrise énergétique, alors que la demande liée à l'IA et aux méthodes de calcul traditionnelles exerce une pression croissante sur l'approvisionnement mondial en électricité.

Au-delà de l'efficacité énergétique, l'amélioration de la modélisation climatique, de la gestion des réseaux et l'émergence de matériaux durables et supraconducteurs issus de la recherche quantique amplifient leur potentiel environnemental.

3.1.16



Q : Comment le Canada se compare-t-il aux autres pays dans ce domaine ?



De façon remarquable. Le Canada est reconnu comme un leader mondial en science quantique et comme un pays dont l'expertise, les industries et le niveau de préparation quantiques dépassent largement son poids relatif. Porté par la vision de scientifiques, d'entrepreneurs et de décideurs publics, le pays dispose d'un écosystème dynamique d'entreprises en technologies quantiques²⁵, de programmes éducatifs matures et reconnus, ainsi que de l'une des plus fortes densités de PME quantiques par habitant²⁶ à l'échelle mondiale. Le Canada compte aussi parmi les rares pays dotés d'un plan national coordonné en sécurité quantique, et le programme de l'Institut canadien de recherches avancées (CIFAR) a joué un rôle clé dans la mise en place de collaborations internationales, permettant au Canada d'influencer l'agenda quantique mondial.

Cette avance initiale est réelle, mais elle n'est pas sans précédent (aérospatiale, télécommunications, IA). En matière de commercialisation, la concurrence est vive face à des acteurs de taille supérieure, comme les États-Unis, la Chine et l'Union européenne.

Préserver et valoriser le travail de ceux qui ont bâti ces fondations et su saisir l'opportunité de cette avance requiert votre engagement actif au sein de l'écosystème, afin de convertir cet avantage en bénéfices économiques durables et tangibles et, à terme, en influence politique.

Voir l'annexe pour une liste d'entreprises canadiennes développant des ordinateurs quantiques.

3.1.17



Q : Comment les pionniers créent-ils un avantage concurrentiel ?

Les pionniers prennent l'avantage en apprenant plus tôt, en anticipant, et en sécurisant rapidement des ressources rares, talents, partenariats et propriété intellectuelle, avant que le marché ne se referme. Leur avance leur permet d'influencer les standards, les conditions d'achat et les feuilles de route de l'écosystème en leur faveur.

Une intégration précoce et des contrats structurants consolident leur crédibilité et ancrent des relations avec des fournisseurs rares, ralentissant les concurrents. Un leadership reconnu renforce la confiance des régulateurs, des clients et des investisseurs, libérant autorisations et capital de confiance pour accélérer l'exécution.

Dans le quantique, ces avantages sont amplifiés par la nouveauté des technologies. À la différence de l'IA, qui a pu s'étendre sur des infrastructures existantes, le quantique ne dispose d'aucune base installée. C'est l'équivalent de construire des rails entièrement nouveaux plutôt que d'ajouter des trains.

²⁴ Energy-Consumption Advantage of Quantum Computation, Florian Meier, Hayata Yamasaki

²⁵ Dans son Quantum Technology Monitor de juin 2025, McKinsey classe le Canada au deuxième rang, derrière les États-Unis, pour le nombre de startups en technologies quantiques.

²⁶ Voir le [site web](#) de Industrie quantique canada

3.1.18



Q : Pourquoi le secteur financier doit-il mener la transition quantique ?

Peu de secteurs sont aussi bien positionnés, aussi fortement motivés ou aussi clairement tenus de jouer un rôle de chef de file mondial dans le développement des capacités quantiques et l'établissement des standards que le secteur financier, et les banques en particulier. Voici pourquoi :

Ils sont à haut risque

La valeur stratégique de leurs données et leur connectivité mondiale placent les banques en tête des cibles des premières attaques quantiques. Leur forte interconnexion signifie qu'une seule brèche cryptographique majeure peut rapidement contaminer tout le réseau financier.

Les banques doivent protéger leur réputation

La préparation au quantique est un marqueur de maturité opérationnelle, de leadership technologique et d'excellence en gouvernance, exactement ce que visent la plupart des banques.

Les banques disposent de l'expertise nécessaire

Le secteur bancaire est historiquement lié à la physique. Les banques emploient des physiciens en modélisation financière, particulièrement en gestion des risques et opérations de marché, et exploitent de vastes infrastructures cryptographiques.

Les banques sont au cœur du réseau mondial de confiance numérique

Par la compensation, le règlement et les marchés des capitaux, les banques sont numériquement connectées à l'ensemble du système financier. Cette interdépendance leur donne la portée systémique nécessaire pour imposer des normes à l'échelle mondiale.

Les banques ont une solide expérience de la coordination mondiale

Le secteur bancaire est mondialement réglementé et déjà tenu d'agir pour garantir sa résilience. Ces autorités disposent aussi des leviers nécessaires pour aligner et diffuser les exigences applicables à l'ensemble des banques.

Ce que font les banques devient rapidement la norme

Toutes les banques sont tenues de respecter la réglementation bancaire, et de nombreux secteurs s'y alignent par effet d'entraînement. Leur influence est majeure. Lorsque les grandes banques imposent des exigences de conformité post-quantique dans leurs contrats fournisseurs, tout l'écosystème suit.

Le changement est porteur d'opportunités

Au-delà de la simple mitigation des risques, les premiers acteurs financiers capteront un avantage stratégique tangible : des modèles de risque plus précis pour mieux piloter le capital, des portefeuilles optimisés offrant de meilleurs rendements ajustés au risque, et de nouveaux produits quantum-secure — tels que des portefeuilles post-quantiques ou des services de vérification de transactions — renforçant la confiance des clients et des partenaires.

Des institutions comme Banco Santander incarnent le leadership prospectif requis pour mener le secteur financier dans la transition quantique, par des partenariats actifs, le développement de capacités internes, l'influence sur les standards mondiaux et le partage ouvert des connaissances.

3.1.19



Q : Pourquoi les standards sont-ils essentiels ?

Dans les technologies émergentes, les standards transforment les avancées scientifiques en systèmes utilisables, interopérables et viables commercialement. Ils fixent un langage commun, des métriques et des protocoles d'interface, permettant aux dispositifs, algorithmes et mécanismes de sécurité de différents acteurs de fonctionner ensemble de manière fiable. En leur absence, l'écosystème quantique s'expose à la fragmentation, à l'incompatibilité et à une perte de confiance.

Les standards ne sont pas uniquement techniques. Ils couvrent aussi des concepts comme les échéanciers de migration et les sources d'information faisant autorité. Ensemble, ils rendent possible une transition coordonnée vers la quantique et cryptographie post-quantique, plutôt que des réponses désordonnées.

Participer activement au développement des standards assure que les besoins et réalités de votre organisation, et de notre pays, sont intégrés aux règles

3.1.20



Q : Pourquoi la souveraineté est-elle cruciale à l'ère quantique ?

La souveraineté est la capacité de décider de manière autonome et de garder le contrôle sur ce qui est essentiel à votre organisation et à notre intérêt national. Elle se décline en plusieurs dimensions et est particulièrement critique dans le contexte du calcul quantique.

La souveraineté numérique est une préoccupation de longue date. Elle renvoie à la capacité de contrôler, gouverner et protéger les données, mais aussi les identités et interactions numériques. Elle répond à une question clé : nos données, identités numériques et infrastructures numériques sont-elles sécurisées, privées et réellement sous notre contrôle ? Elle englobe les cadres d'identité, la résidence des données et l'intégrité de l'authentification. Fondamentalement, elle vise à préserver la confiance numérique.

La souveraineté technologique est la capacité de développer, maîtriser et faire évoluer nos technologies critiques incluant le matériel, logiciels, chaînes d'approvisionnement, ainsi que les capacités de recherche et développement. La question centrale est simple : pouvons-nous bâtir ou nous approvisionner de façon fiable sans créer de vulnérabilité stratégique ? À l'ère quantique, cela englobe les technologies quantiques, la cryptographie post-quantique et leurs technologies habilitantes clés (systèmes cryogéniques, lasers),

Le niveau de souveraineté numérique et technologique conditionne notre résilience et notre aptitude à convertir notre leadership et le capital intellectuel quantiques en puissance économique future.

3.1.21



Q : Peut-on expérimenter les technologies aujourd'hui ?

Oui. Des infrastructures, plateformes et partenariats sont déjà disponibles pour expérimenter, développer des compétences et explorer des cas d'usage sans posséder de matériel ni engager d'investissements majeurs, et le Canada offre l'un des environnements les plus concrets au monde pour apprendre en faisant.

Notre écosystème est exceptionnellement riche en entreprises quantiques, en expertise et en recherche appliquée. Plusieurs entreprises offrent l'accès commercial à de véritables ordinateurs quantiques, ainsi que de la formation pratique, souvent gratuit. Des possibilités d'expérimentation avec des cas d'usage et conditions réelles sont également offertes par nos institutions et programmes universitaires de calibre international, dont le *Pôle de recherche en finance quantique* de l'Université de Sherbrooke.

En matière de préparation post-quantique, le Canada bénéficie aussi d'un avantage unique avec Kirq, un organisme sans but lucratif qui exploite un banc d'essai ouvert qui réunit des systèmes classiques et quantiques en conditions opérationnelles réelles, avec un large éventail de technologies et de produits accessibles à l'expérimentation.

Ensemble, ces capacités permettent à nos organisations de renforcer leur expertise quantique interne, tester des technologies sous de vraies contraintes opérationnelles, et accélérer leur transition vers des solutions résilientes à l'ère quantique, le tout avec un investissement minimal et un risque fortement réduit.

Votre feuille de route quantique



La chance n'est pas une stratégie -*Michele Mosca*

La préparation quantique n'est pas fortuite. Elle requiert une stratégie et une planification disciplinée. Cette section propose une feuille de route pour développer les capacités, la gouvernance et les protections clés afin de sécuriser votre organisation et de l'ancrer clairement dans le quadrant visé de Boussole de l'urgence

4.1

Principes directeurs

Les principes directeurs assurent des décisions cohérentes et des priorités pertinentes, malgré l'évolution du contexte et des circonstances.

Nous retenons les principes suivants :

Ancrer dans la raison d'être et le risque

La feuille de route, ainsi que vos indicateurs clés de performance et de progression, doivent refléter et suivre votre avancement selon les trois dimensions suivantes :

- 1 **Devoir fiduciaire** : leadership et gouvernance face au changement
- 2 **Posture de risque** : le quantique comme menace à la sécurité
- 3 **Compétitivité à long terme** : le quantique comme futur levier d'avantage

Rendre la sécurité non négociable

Le risque doit précéder la récompense. Priorisez l'atténuation des menaces pour protéger les données, maintenir la confiance et affirmer une gouvernance responsable, malgré l'évolution des menaces et des normes.

Bâtir des capacités durables

Dépassez les actions ponctuelles et les pilotes. Déployez la cryptoagilité et intégrez la mitigation des menaces cryptographiques au quotidien, pas sur un horizon de 30 ans. Investissez dans la littérature quantique, la gouvernance, les compétences et la gestion des fournisseurs pour créer une capacité durable qui s'amplifie avec le temps.

Ensemble, nous sommes plus forts

Les enjeux sont considérables, peut-être plus élevés qu'ils ne l'ont jamais été. Face aux questions de confiance numérique mondiale et de souveraineté nationale, nous avons davantage à gagner en travaillant ensemble qu'en agissant en ordre dispersé. Que votre stratégie quantique soit guidée par la collaboration avec vos pairs de l'industrie plutôt que par une posture strictement concurrentielle.

Agir avec certitude, sans renoncer à l'optionnalité

Votre plan doit conjuguer flexibilité et certitude. Les règles diffèrent selon le flux dans lequel vous agissez. Commencez par comprendre où et pourquoi chacune est requise.

Avancer avec une certitude cryptographique

En cryptographie, les normes sont primordiales. Les systèmes cryptographiques robustes ne sont pas solides parce qu'ils sont secrets, mais parce qu'ils ont été examinés publiquement, testés et éprouvés par la communauté cryptographique mondiale. Traitez votre architecture cryptographique comme le socle de votre écosystème. Respectez les normes établies et privilégiez les outils les plus robustes et les plus complets disponibles.

Avancer avec l'optionnalité des architectures de qubits

Il est trop tôt pour déterminer quelles technologies de calcul quantique s'imposeront comme normes de marché, et toutes les capacités ne sont pas transférables d'une architecture de qubits à l'autre. Diversifiez vos partenaires et vos technologies à mesure que vous explorez les usages du quantique afin d'éviter de vous retrouver en marge des standards émergents.

Penser globalement, agir localement

Engagez-vous à l'échelle mondiale pour influencer la réglementation et les normes, tout en investissant localement afin de développer les talents, stimuler l'innovation, protéger la souveraineté et renforcer la résilience des chaînes d'approvisionnement, des partenariats et des infrastructures locales.

4.2

Années 0–1 : posture de risque imminente

Toutes les actions présentées ci-dessous sont conçues pour être menées en parallèle.

4.2.1

Rester informé en continu

Former votre conseil d'administration et vos dirigeants

Concevez et offrez aux conseils et aux dirigeants des formations sur les risques et opportunités du quantique²⁷.

- En raison de leur responsabilité fiduciaire, les membres des conseils d'administration constituent un levier clé pour s'assurer que la direction agit avec l'urgence appropriée.
- Un conseil informé et engagé est un puissant différenciateur stratégique en période de disruption.

Mettre en place un programme de reddition de comptes rigoureux

Maintenez la direction et le conseil informés, et imposez à l'équipe de livraison une reddition de comptes fondée sur une information claire et pertinente.

- Faites de la migration PQC un programme approuvé par le conseil, explicitement ancré dans le devoir fiduciaire.
- Définissez clairement l'information servant au suivi de votre progression et celle qui doit être présentée au conseil d'administration.
- Un mécanisme de reddition de comptes bien conçu est le meilleur moyen de maintenir l'accent sur les bonnes priorités et d'investir vos ressources là où elles génèrent le plus de valeur et d'impact.

Faire le bilan des leçons apprises

L'ère de l'IA a démontré le prix d'une accélération sans gouvernance. L'ère quantique impose anticipation et maîtrise. Tirez parti de votre expérience en AI Readiness pour bien faire les choses dès le départ.

- Où avez-vous réussi ou échoué dans votre stratégie et votre préparation à l'IA : gouvernance, gestion des risques, talents, processus, décisions, données, leadership ?
- Appuyez-vous sur votre expérience pour adopter une approche de préparation quantique plus intentionnelle et prospective, conçue pour agir stratégiquement et positionner votre organisation en leader plutôt qu'en suiveur.



Pourquoi cela importe

Les prochaines années seront tumultueuses. Sans un leadership informé et une reddition de comptes rigoureuse, les organisations risquent de sous-estimer la vitesse du changement et de manquer des fenêtres critiques pour protéger leurs actifs.

Un conseil d'administration formé constitue un atout stratégique en période de disruption. Un conseil bien informé agit à la fois comme mécanisme de pilotage et comme accélérateur. S'assurer qu'il est pleinement préparé renforce la capacité de votre organisation à réagir rapidement en situation de crise.

²⁷ Ce guide fournit un cadre efficace et les contenus essentiels servant de base à cette formation.

Mettre en place une « équipe de préparation quantique »

La préparation quantique est multidimensionnelle et requiert une action concertée entre disciplines. Pour éviter une approche fragmentée ou en silos, vous devez mettre en place une structure cohérente permettant de consolider l'expertise et de coordonner votre réponse. Le *modèle de préparation quantique* illustre le type d'organisation requis.

- Au cœur du modèle se trouve votre *équipe de préparation quantique*, qui rassemble des experts et des leaders issus de la stratégie d'affaires, des TI, du risque, de la cybersécurité et de l'analytique afin de piloter votre stratégie quantique et de coordonner la préparation de l'organisation.
- Ils travaillent ensemble pour capter et partager les connaissances, maintenir l'alignement sur les échéances et les impératifs clés, tout en conservant deux axes de concentration distincts :
 - **Axe sécurité post-quantique** : piloté par le Chef de la sécurité de l'information (CISO) et tenu responsable de l'élaboration et de la mise en œuvre de votre stratégie défensive.
 - **Axe avantage quantique** : piloté par le Chef de l'analytique (CAO) et tenu responsable de l'élaboration et de la mise en œuvre d'une stratégie de création de valeur inspirée du quantique.

→ **Disposez-vous d'experts en physique ou en mathématiques au sein de votre organisation ?** Les physiciens séparent le signal du bruit quantique et identifient des cas d'usage à forte valeur, tout en challengeant les promesses fournisseurs irréalistes. Les mathématiciens, experts en cryptographie, soutiennent vos équipes de cybersécurité dans l'évaluation des options résistantes au quantique et des risques de transition. Ensemble, ils aident à poser les bonnes questions, valider les hypothèses et guider les dirigeants vers des décisions fondées sur la réalité technique plutôt que sur le marketing. De nombreuses institutions financières disposent déjà de ces compétences, notamment en gestion des risques et en négociation.

? Pourquoi cela importe

La préparation quantique relève d'une transformation multidisciplinaire, non d'un projet unique. Sans structure coordonnée, les efforts se dispersent, les synergies se perdent et l'imputabilité s'affaiblit. Le modèle de préparation quantique apporte cohérence et momentum.

Le modèle de préparation quantique

Un programme de préparation efficace repose sur une organisation rigoureuse. Le schéma ci-dessous présente le modèle de gouvernance cible.



Mandater une évaluation de haut niveau des risques et des opportunités

L'objectif est d'obtenir une première vision approximative des enjeux propres à votre organisation.

- ➔ Votre **analyse de l'exposition aux risques** doit couvrir à la fois les menaces cyber et les menaces de marché, y compris les risques de disruption des marchés et les impacts à l'échelle mondiale.
- ➔ Votre **évaluation des opportunités** doit identifier les principaux cas d'usage du calcul quantique pour votre secteur et pour votre organisation.

Déterminer les délais de préparation

En vous appuyant sur les informations de votre équipe de préparation quantique :

- ➔ Fixez votre date cible de préparation selon votre exposition aux risques. Les organisations dont les actifs confidentiels à longue durée de vie sont fortement exposés devront accélérer.
- ➔ Identifiez les signaux indiquant que cette échéance approche ou évolue, et mettez en place les mécanismes nécessaires pour la mettre à jour régulièrement.

S'aligner sur votre intention défensive

Identifiez le quadrant de la Boussole d'urgence visé pour votre organisation au Q-Day.

- ➔ Développez un discours clair sur ce que cela implique et assurez-vous qu'il soit intégré à l'appétence au risque de l'entreprise, aux priorités stratégiques et aux communications avec les régulateurs, les investisseurs et les employés.

Définir votre feuille de route défensive

Elle doit inclure deux flux de réalisation distincts mais interconnectés.

- 1 Un flux visant à développer la cryptoagilité au sein de votre organisation, incluant :**
 - ➔ Une évaluation de la maturité des capacités et des écarts de capacité.
 - ➔ Des actions ciblées pour renforcer les capacités et combler les écarts, couvrant le modèle opérationnel, les compétences, la capacité, la formation, les processus et les outils durables.
- 2 Un flux visant à compléter votre migration vers la cryptographie post-quantique, incluant :**
 - ➔ Un inventaire des usages de la cryptographie à l'échelle de l'entreprise, incluant la complexité et l'effort associés à la migration de chaque instance, ainsi que les délais estimés de réalisation.
 - ➔ Une évaluation des dépendances cryptographiques auprès des fournisseurs externes et des infrastructures critiques de tiers, accompagnée d'un plan pour évaluer leur niveau de préparation et leur conformité.
 - ➔ Une priorisation des actifs critiques par phases (systèmes prioritaires d'abord, puis actifs à risque moindre).
 - ➔ Les hypothèses de base, les ressources requises et les échéanciers de migration.

Allouer des budgets

- Traitez la migration vers la cryptographie post-quantique non comme un projet ponctuel, mais comme un programme d'investissement pluriannuel et un besoin opérationnel de long terme, soutenu par des capacités étendues de cryptoagilité.
- Incluez des catégories budgétaires couvrant l'inventaire cryptographique, les outils de migration, la formation de la main-d'œuvre, les contrats fournisseurs et les tests indépendants.



Pourquoi cela importe

Atteindre la préparation quantique exige une compréhension partagée au sein du leadership de ce qui doit être fait, quand et pourquoi. Comprendre à la fois l'exposition (vos vulnérabilités) et les opportunités (vos leviers de gain) est essentiel pour fixer des priorités et des échéanciers réalistes. Une cible et un calendrier communs permettent d'aligner stratégie, ressources et imputabilité autour d'un plan d'action unifié.

4.2.5

Sécuriser les partenaires externes

Engager des guides et partenaires stratégiques

Le moment est venu de sécuriser une expertise externe, car la demande augmentera rapidement à mesure que la prise de conscience s'accroît et que le Q-Day approche. Recherchez des firmes et des individus disposant d'une expérience en gestion des risques TI, en cybersécurité et en transformations numériques à grande échelle, ainsi que d'une connaissance approfondie et de relations au sein de votre écosystème local.

4.2.6

Mettre en place le suivi des politiques et de la conformité

Mettre à jour les politiques et les processus

- **Exiger que tous les fournisseurs** fournissent des feuilles de route PQC dans les contrats et les appels d'offres.
- **Actualiser le suivi des risques** en intégrant les jalons de migration PQC aux registres des risques, aux audits et aux cycles de renouvellement TI.
- **Assurer l'alignement avec l'appétence au risque** de l'entreprise, incluant les exigences de reporting ESG et de résilience, ainsi que les attentes réglementaires.

4.3

Années 1-2 : Expérimentation et montée en capacité

4.3.1

Développer votre stratégie quantique – usage stratégique

- **Identifiez les cas d'usage prioritaires** à forte valeur d'affaires et au potentiel mesurable.
- **Sécurisez un financement et des ressources dédiés** afin d'assurer la continuité et la réalisation.
- **Mettre en place une fonction de suivi** pour mesurer la performance des cas d'usage.
- **Fixez une vision et des balises** à travers un énoncé prospectif (p. ex. : D'ici le Q-Day, nous pourrions...).

4.3.2

Prioriser et financer votre stratégie

- ➔ Appliquez les principes directeurs pour évaluer les opportunités et les risques concurrents des cas d'usage activés par le quantique.
- ➔ Sélectionnez les priorités clés (X initiatives) alignées sur les objectifs stratégiques et la capacité disponible.

4.3.3

Bâtir pour le long terme

Évaluez la maturité et les besoins de votre organisation pour l'ère quantique.

- ➔ Déterminez les capacités requises et les écarts à combler sur toutes les dimensions, incluant :
 - ➔ Partenariats stratégiques : avec des entreprises, des fournisseurs, des universités et des groupes sectoriels.
 - ➔ Expertise : clarifier les compétences à développer ou à sourcer.
 - ➔ Gouvernance : définir les rôles, les droits décisionnels, les considérations de souveraineté et établir des indicateurs de performance et de risques.
 - ➔ Données : accès sécurisé, qualité et disponibilité pour les cas d'usage quantiques et hybrides.
 - ➔ Personnes : recrutement, développement et programmes de formation transverses.
 - ➔ Processus : la sélection des cas d'usage, l'évaluation des risques et l'allocation des fonds.
- ➔ Élaborez des stratégies pour combler les écarts
- ➔ Clarifiez l'imputabilité de chaque initiative et faites approuver le financement par le conseil.

4.4

Années 3-5 : Avantage stratégique

À cet horizon, le plan s'allège — comme il se doit. La volatilité actuelle limite la visibilité à long terme.

Si vous avez suivi ce plan et respecté vos principes, vous disposerez néanmoins d'une position nettement plus favorable que la plupart.

Considérations clés pour cette période

- ✓ Poursuivez un suivi étroit et un soutien actif de votre plan de migration vers la cryptographie post-quantique.
- ✓ Capitalisez sur le travail préparatoire réalisé lors des tests de vos cas d'usage quantiques.
- ✓ Prenez soin de votre bassin de talents et protégez-le.
- ✓ Assurez l'entretien continu des écosystèmes de partenaires et des alliances.
- ✓ Maintenez des collaborations sectorielles actives et contribuez à l'évolution des normes.
- ✓ Intégrez l'avantage quantique à votre modèle d'affaires.
- ✓ Préparez-vous à mesurer votre retour sur investissement et la valeur à long terme.
- ✓ Captez les leçons apprises de votre démarche de préparation quantique.

Annexes et outils

Glossaire des termes

Terme	Définition
Cryptoagilité	La capacité de mettre à jour ou de remplacer rapidement les systèmes cryptographiques à mesure que de nouveaux algorithmes, menaces ou standards émergent.
Confiance numérique	La confiance que les interactions et transactions numériques sont sécurisées, authentiques et fiables à travers des systèmes interconnectés.
Ordinateur quantique tolérant aux fautes	Un ordinateur quantique entièrement corrigé des erreurs, capable d’exécuter de manière fiable des calculs longs et complexes, marquant le seuil d’une utilisation commerciale à grande échelle.
Devoir fiduciaire	L’obligation des conseils et des dirigeants d’anticiper et de maîtriser les risques et opportunités quantiques émergents afin de préserver la valeur des parties prenantes, l’intégrité des données et la confiance du public.
Harvest Now, Decrypt Later (HNDL)	Un modèle de menace dans lequel des données chiffrées sont volées aujourd’hui afin d’être déchiffrées ultérieurement, lorsque des ordinateurs quantiques seront capables de briser les mécanismes de chiffrement actuels.
Trust Now, Forge Later (TNFL)	Un scénario de menace connexe dans lequel des attaquants capturent aujourd’hui des données d’authentification afin de forger ultérieurement des identifiants valides une fois la cryptographie compromise.
Internet of Things (IoT)	Désigne le réseau d’objets physiques du quotidien intégrant des logiciels et une connectivité, leur permettant de collecter, d’échanger et d’exploiter des informations sur Internet sans intervention humaine directe.
NISQ (Noisy Intermediate-Scale Quantum)	La génération actuelle de dispositifs quantiques, caractérisée par un nombre limité de qubits et des taux d’erreur élevés, utile pour la recherche et l’expérimentation, mais pas encore pour des applications critiques.
Cryptographie post-quantique (PQC)	Algorithmes cryptographiques conçus pour résister aux attaques des ordinateurs quantiques tout en demeurant compatibles avec les systèmes numériques actuels.
Operational Technology (OT)	L’interconnexion des technologies industrielles, telles que celles utilisées dans les usines de fabrication, les réseaux énergétiques, les systèmes ferroviaires ou les installations de traitement de l’eau. Elle repose généralement sur des réseaux propriétaires, qui ne sont toutefois pas toujours entièrement isolés de l’Internet public.
Infrastructure à clés publiques (PKI)	L’ensemble des technologies, politiques et processus qui gèrent les certificats numériques et les clés de chiffrement afin de sécuriser les identités, les communications et les transactions.
Q-Day	Le jour où les ordinateurs quantiques deviendront suffisamment puissants pour briser les mécanismes de chiffrement à clé publique actuels, exposant des données sensibles et des communications à l’échelle mondiale.
Avantage quantique	Le point à partir duquel un ordinateur quantique surpasse les meilleurs ordinateurs classiques pour une tâche précise et concrète.
Maturité des capacités quantiques	Une mesure du degré d’avancement des structures, des compétences et de la gouvernance d’une organisation dans l’intégration des enjeux quantiques à la stratégie et aux opérations.
Équipe de préparation quantique	Une petite équipe transversale chargée de surveiller les avancées quantiques, d’en évaluer les impacts et de coordonner les initiatives de préparation.
Écosystème quantique	Le réseau de gouvernements, d’institutions de recherche, de jeunes entreprises et de grandes organisations collaborant à l’avancement de la science quantique et à sa commercialisation.

Term	Definition
Distribution quantique de clés (QKD)	Une méthode d'échange sécurisé de clés fondée sur la physique quantique, dans laquelle toute tentative d'interception est immédiatement détectable et corrigible.
Littératie quantique	La compréhension fondamentale des concepts quantiques requise pour permettre aux dirigeants de prendre des décisions stratégiques et de gestion des risques éclairées.
Préparation quantique	Le degré selon lequel une organisation comprend, anticipe et se dote des capacités nécessaires pour gérer à la fois les risques et les opportunités liés aux technologies quantiques.
Souveraineté quantique / technologique	La capacité d'un État ou d'une organisation à développer, contrôler et sécuriser des technologies quantiques critiques sans dépendre d'entités étrangères.
Cas d'usage quantique	Une application concrète dans laquelle le calcul quantique ou les capteurs quantiques offrent un avantage mesurable par rapport aux méthodes classiques.
IA améliorée par le quantique	Des systèmes d'intelligence artificielle qui exploitent des algorithmes quantiques ou du matériel quantique afin d'accélérer l'apprentissage, l'optimisation ou la résolution de problèmes.
Qubit	L'unité fondamentale de l'information quantique ; contrairement à un bit classique, un qubit peut exister simultanément dans plusieurs états, permettant dans certains cas un calcul massif en parallèle.
Architecture de qubits	La conception physique et d'ingénierie utilisée pour construire les qubits, comme les circuits supraconducteurs, les ions piégés ou les systèmes photoniques, chacun présentant des compromis de performance distincts.
Boussole de l'urgence	Un cadre visuel illustrant l'interaction entre le niveau de préparation et le moment d'action, et montrant les résultats associés à une action précoce par rapport à un retard de réponse.

5.2

Notes explicatives sur des concepts sélectionnés

5.2.1

Autres technologies quantiques

Le calcul quantique n’est qu’une des catégories de technologies quantiques. La section suivante présente un bref aperçu des deux autres catégories.

Capteurs quantiques

Les capteurs quantiques exploitent les propriétés fondamentales de la mécanique quantique pour détecter et mesurer des variations extrêmement faibles de grandeurs physiques (temps, gravité, température, champs magnétiques et électriques), avec un niveau de précision et de sensibilité inatteignable pour les capteurs classiques. Les capteurs quantiques avancés génèrent déjà des bénéfices concrets en médecine, en découverte de matériaux et dans la vie quotidienne. En mobilisant des effets quantiques, ils ouvrent de nouvelles façons d’observer le monde, en détectant des variations infinitésimales de la gravité, des champs électromagnétiques, de la température, de la pression ou du mouvement. Plusieurs produits fondés sur des technologies de détection quantique sont aujourd’hui matures et pleinement commercialisés. Par exemple, les gravimètres et accéléromètres quantiques basés sur l’interférométrie à atomes froids permettent une navigation ultra-précise et la cartographie de ressources souterraines sans GPS. Les magnétomètres quantiques à base de diamant peuvent détecter de très faibles champs magnétiques générés par l’activité électrique du cœur ou du cerveau, ouvrant la voie à de nouvelles techniques de diagnostic médical et à des avancées majeures en recherche scientifique.

Communications quantiques (QKD)

La distribution quantique de clés est une technologie fondée sur le quantique qui utilise du matériel spécialisé et les principes de la physique quantique pour distribuer de manière sécurisée des clés de chiffrement entre des sites physiques. Elle est considérée comme très sécuritaire et non vulnérable aux attaques d’ordinateurs quantiques ou classiques. Toutefois, des obstacles technologiques subsistent et il n’existe pas de trajectoire claire vers une adoption à grande échelle comme substitut direct aux méthodes de chiffrement actuelles. Elle demeurera une technologie cryptographique complémentaire, à usage limité, tant que ces barrières ne seront pas levées à l’échelle industrielle.

5.2.2

Vue d’ensemble des risques

Perte d’opportunités (impact concurrentiel et missionnel)

Ce que c’est

Prendre du retard pendant que vos pairs sécurisent les talents, la PI, les partenaires et les accès de premier plan, et préparent leur organisation à tirer parti de cette nouvelle technologie ; manquer les premiers gains se traduit ensuite par des courbes d’apprentissage plus lentes et des coûts plus élevés.

Pourquoi cela importe

Croissance réduite, marges affaiblies et crédibilité amoindrie auprès des clients et des investisseurs ; recrutement et rétention des meilleurs talents plus difficiles.

Signaux de risque

Aucun sponsor exécutif, aucune stratégie quantique, aucun projet pilote financé, aucun portefeuille de cas d’usage quantiques priorisés par la valeur ; posture passive au sein des consortiums de normalisation.

Risque d'exposition (sécurité et conformité)

Ce que c'est

Les risques directs pour votre organisation incluent l'exposition de vos actifs de données, l'augmentation des cyberattaques et de la fraude. La non-conformité des tiers et des fournisseurs aux standards de cryptographie post-quantique amplifie ces risques. À l'échelle de l'écosystème mondial, les risques comprennent la dégradation de la confiance numérique qui sous-tend l'usage d'Internet.

Pourquoi cela importe

La confiance et l'authentification des tiers sont au cœur de toute activité numérique. Leur rupture entraîne des violations de confidentialité, une perte d'intégrité des données et l'interruption des canaux et transactions numériques. Le scénario favorable se traduit par des pénalités réglementaires et des litiges ; le pire met en péril vos opérations et a des répercussions économiques et politiques mondiales. Les fenêtres d'exposition dureront des années et sont déjà actives via « Harvest now, decrypt/forged later ».

Signaux de risque

La direction est incapable de produire un inventaire fiable et détaillé des clés cryptographiques, lié aux processus d'affaires et TI qui les utilisent. Les contrats avec les fournisseurs et partenaires ne comportent pas de clauses imposant l'adoption de la cryptographie post-quantique, et aucun processus n'est en place pour valider la conformité de votre organisation ou de vos fournisseurs. Manque d'urgence ou de mobilisation à l'échelle mondiale. Développement plus rapide que prévu des ordinateurs quantiques tolérants aux fautes.

Risque de souveraineté (contrôle des capacités critiques)

Ce que c'est

Dépendance stratégique à l'égard de matériel étranger, d'accès au cloud, de bibliothèques, de standards et de talents rares ; contraintes liées à la résidence des données et aux contrôles à l'exportation ; écosystème quantique national fragmenté ou immature.

Pourquoi cela importe

Perte de pouvoir de négociation, hausse des coûts, accès plus lent et vulnérabilité accrue aux chocs géopolitiques. Pour le secteur public et la finance réglementée, cela peut compromettre l'exécution des missions et les priorités nationales.

Signaux de risque

Dépendance à un fournisseur unique, PI critique détenue sous conditions partenaires, absence d'écosystème local (programmes publics, formation académique, liens recherche-industrie) et posture ambiguë sur la résidence des données, hébergées à l'étranger ou sous contrôle d'entités étrangères.

5.2.3

Types d’architectures de qubits

Les qubits peuvent adopter différentes architectures physiques. Chaque architecture cible un phénomène quantique précis et se distingue fondamentalement des autres.

Comprendre les architectures de qubits n’est pas indispensable, mais constitue un avantage déterminant pour les premiers entrants. D’autant plus que les actifs et compétences développés pour une architecture donnée sont rarement transférables à une autre.

Lorsque vous évaluez les architectures de qubits, pensez matériel distinct, bassins de talents distincts, chaînes d’approvisionnement distinctes et jalons logiciels distincts.

À titre d’exemple, sur le plan opérationnel, les qubits supraconducteurs exigent des avancées en réfrigération par dilution, les pièges à ions requièrent des chambres à ultra-haut vide, et les qubits photoniques nécessitent de meilleurs émetteurs et détecteurs de photons uniques. Chacun de ces besoins représente en soi une opportunité industrielle.

Sans entrer dans les détails techniques, il est essentiel de comprendre que les feuilles de route diffèrent selon les architectures et que leur comparaison ne peut se faire de manière naïve.

Comme pour toute technologie émergente, une fois la maturité atteinte, ces architectures ne seront plus une préoccupation pour les utilisateurs finaux et les organisations. Cela dit, la compréhension de l’ensemble du paysage architectural demeure clé pour établir un avantage de premier entrant, du positionnement dans la chaîne d’approvisionnement à l’acquisition de talents.

Nous recommandons de prendre le temps d’analyser chaque approche et la position des acteurs de l’écosystème ciblé.

5.2.4

Fournisseurs canadiens d’ordinateurs quantiques

Nom de l’entreprise / Emplacement	Architecture de qubits	Facteurs distinctifs de leur approche <i>(texte non traduit pour assurer l’intégrité scientifique)</i>
Nord Quantique Sherbrooke, QC	Superconducting	Using bosonic modes held in cavities to enable error correcting qubits without requiring physical redundancy. Building fault-tolerant quantum computers that are efficient and useful for a wide variety of applications.
Xanadu Toronto, ON	Photonic	Using photons as qubits encoded in integrated photonic chips and optical circuits, enabling modular quantum computing with high connectivity and near-room-temperature operation.
D-Wave Vancouver, BC (now global)	Superconducting	Using a specialized type of quantum computing, called quantum annealing. Using superconducting qubits to find solutions to complex optimization problems by naturally settling into the lowest-energy state.
Anyon Montreal, QC	Superconducting	Proprietary quantum hardware including modular quantum processors, cryogenic systems, and quantum control electronics using superconducting qubits (similar to IBM or Google's approach)
Photonic, Inc. Vancouver, BC	Photonic	Quantum computing platform based on silicon spin qubits ("T centers")that are connected through photonics Their approach combines three key elements: computing (using spin qubits), networking (via photons), and memory.
Open Quantum Design Waterloo, ON	Trapped ions	Non-for-profit organization committed to radical transparency and full-stack open access, with a Trapped-Ion Architecture as a core technology: Individual ions as qubits, held in place by electromagnetic traps in a vacuum and manipulated with precise lasers.

5.2.5

Internet des objets (IoT)

L'internet des objets (IoT) désigne le réseau d'objets physiques, tels que les appareils, capteurs, véhicules et machines, intégrant des logiciels leur permettant de collecter, d'échanger et d'exploiter des informations via l'internet, sans intervention humaine directe.

Voici des exemples d'applications de l'IoT, réparties par domaines d'usage :

Maisons intelligentes

- ✓ Thermostats à ajustement automatique de la température (ex. Nest)
- ✓ Éclairage intelligent adaptatif selon l'occupation ou la luminosité
- ✓ Assistants vocaux comme Amazon Echo ou Google Home
- ✓ Systèmes d'alarme et de vidéosurveillance résidentiels

Santé

- ✓ Capteurs portables et montres intelligentes pour le suivi de la fréquence cardiaque et de l'activité
- ✓ Dispositifs de suivi à distance des patients chroniques
- ✓ Distributeurs intelligents de médicaments pour le suivi de l'adhésion thérapeutique

Transport

- ✓ Véhicules connectés transmettant des données de diagnostic et soutenant la maintenance prédictive.
- ✓ Systèmes de gestion de flotte avec suivi GPS en temps réel et optimisation du carburant.

Chaque exemple illustre comment l'IoT relie les mondes physique et numérique, génère des données et offre des capacités qui améliorent l'efficacité, la sécurité des personnes et la prise de décision, tout en créant un point de vulnérabilité lorsque la confiance numérique fait défaut.

La technologie opérationnelle (*Operational technology - OT*)

Proche de l'IoT sur le plan conceptuel, la technologie opérationnelle concerne l'interconnexion de machines industrielles, des usines aux réseaux énergétiques, en passant par le ferroviaire et le traitement de l'eau. Souvent déployée sur des réseaux propriétaires sans être totalement isolée d'Internet, elle demeure exposée en cas de rupture de la confiance numérique.

Exemples de technologie opérationnelle :

Industriel / manufacturier

- ✓ Systèmes de contrôle qualité en temps réel
- ✓ Capteurs de surveillance des vibrations, de la température et de la performance des machines
- ✓ Systèmes de maintenance prédictive
- ✓ Systèmes automatisés d'inventaire et de logistique

Agriculture

- ✓ Capteurs de sol et d'humidité dédiés à l'irrigation de précision
- ✓ Drones intelligents pour le suivi de l'état des cultures
- ✓ Suivi du bétail par colliers connectés

Villes intelligentes

- ✓ Éclairage public connecté
- ✓ Bacs de déchets signalant leur niveau de remplissage
- ✓ Surveillance et contrôle des systèmes de transport

5.2.6

Questions clés supplémentaires pour les dirigeants

Une fois votre posture organisationnelle définie et votre réponse initiale engagée, vous pouvez aborder les questions suivantes :

- 
- Quelles données et quels certificats à longue durée de vie détenez-vous qui pourraient être collectés aujourd'hui puis déchiffrés ou falsifiés plus tard?
 - Quel est le plan de migration vers le PQC de vos tiers, fournisseurs infonuagiques et partenaires clés?
 - Comment réagiriez-vous si une percée quantique survenait plus tôt que prévu?
 - Comment bâtissez-vous l'optionnalité nécessaire pour pivoter lorsque les capacités quantiques mûriront?
 - Quel niveau de dégradation de performance ou de débit êtes-vous prêts à accepter dans le cadre d'une transition PQC?
 - Avez-vous mis en place une gouvernance dédiée à la transition quantique et cryptographique?
 - Quels indicateurs utiliserez-vous pour mesurer la préparation quantique (PQC, inventaire, cas d'usage, exposition au risque)?
 - Quelles obligations réglementaires ou de conformité pourraient exiger une préparation quantique dans vos marchés?
 - Quels modèles d'affaires émergents le quantique pourrait-il activer?
 - Quels signaux ou événements déclencheurs feront basculer l'organisation de la planification à l'exécution?

Questions clés supplémentaires pour les dirigeants



- Contribuez-vous activement à la définition des standards via des consortiums et groupes de travail sectoriels?
- Quels partenaires, chaînes d'approvisionnement ou tiers risquent de devenir des points de faiblesse faute de préparation quantique?
- Quelles alliances stratégiques faut-il nouer dès maintenant avec le milieu académique, les gouvernements et les entreprises quantiques pour vous positionner favorablement?
- Disposez-vous des talents requis en science quantique, informatique quantique et cryptographie post-quantique, ou pouvez-vous les recruter?
- Quelles initiatives de formation et de montée en compétences lancer dès maintenant pour la direction, la sécurité, l'architecture et les opérations?
- Quels partenariats structurants établir avec des universités, laboratoires quantiques et centres de recherche?
- Comment instaurer une culture d'innovation permettant une expérimentation quantique ou hybride sécurisée?
- Quel niveau de risque acceptez-vous pour l'expérimentation quantique de pointe?
- Êtes-vous alignés de façon proactive avec des initiatives nationales ou régionales pour protéger vos intérêts à mesure que les écosystèmes quantiques et d'IA évoluent?
- Quels budgets réserver dès maintenant (R-D, pilotes, matériel, services-conseils)?
- Comment évaluez-vous le rapport coûts-bénéfices? La préparation quantum-safe est-elle un coût d'assurance, un catalyseur ou un facteur de différenciation?
- Quel plan de contingence prévoyez-vous si les échéanciers dérapent ou si des percées quantiques s'accélèrent?

Et la liste n'est pas complète...

Panorama des normes

De multiples initiatives visant l'élaboration de normes en informatique quantique et la réponse au risque quantique sont en cours. Voici un aperçu des plus structurantes du point de vue de la participation canadienne.

A

Normes canadiennes et comités miroirs : comité miroir du SCC pour l'ISO/IEC JTC 3

- L'ISO et l'IEC ont mis sur pied le comité technique conjoint ISO/IEC JTC 3 – Technologies quantiques, chargé de la normalisation des technologies quantiques, de l'informatique et de la simulation quantiques aux sources, détecteurs, communications et à la métrologie.
- Le mandat de ce comité couvre la normalisation de l'ensemble du domaine des technologies quantiques, incluant l'informatique quantique, la simulation quantique, les sources quantiques, les détecteurs, les communications et la métrologie.
- Cela permet aux parties prenantes canadiennes, dont votre organisation, de contribuer aux travaux internationaux de normalisation quantique via le réseau du SCC.

B

Orientations et échéanciers du gouvernement fédéral canadien – Cyber Centre / Secrétariat du Conseil du Trésor du Canada / Services partagés Canada

- Le Cyber Centre canadien a publié une feuille de route pour la migration vers la cryptographie post-quantique des systèmes TI non classifiés du gouvernement du Canada. Elle établit des échéanciers clairs : plan initial d'ici avril 2026, systèmes prioritaires d'ici fin 2031, puis l'ensemble des systèmes d'ici fin 2035.
- Les orientations priorisent une PQC normalisée et exigent une planification de transition appuyée par la gouvernance, l'évaluation des fournisseurs et un inventaire cryptographique. La stratégie du GC positionne la transition « quantum-safe » comme une priorité nationale.

C

Le Forum canadien pour la résilience des infrastructures numériques (CFDIR)

- Le Forum canadien pour la résilience des infrastructures numériques (CFDIR) est une collaboration public-privé volontaire et orientée action visant à renforcer la résilience des infrastructures numériques critiques du Canada, au service d'une économie numérique de confiance et d'un secteur de la cybersécurité solide.
- L'un des groupes de travail du Forum publie chaque année une mise à jour de son rapport sur les meilleures pratiques de préparation quantique afin d'aider les acteurs des infrastructures critiques canadiennes à agir dès maintenant et à planifier la transition de leurs systèmes numériques vers des solutions cryptographiques résistantes au quantique. Le rapport accélère l'apprentissage en fournissant des conseils concrets et des exemples pratiques de mise en œuvre, évitant aux organisations de devoir repartir de zéro.

D

Union internationale des télécommunications (UIT) – Normes de réseaux de distribution de clés quantiques (QKD)

- Exemple de norme publiée : la recommandation ITU-T Y.3800 « Overview on networks supporting quantum key distribution (QKD) » (v1.1, juillet 2020).
- Plus ciblé sur les communications quantiques que sur l'informatique quantique au sens large, cet exemple illustre néanmoins la normalisation quantum-safe et quantum-enabled dans les télécommunications.

Tableau de synthèse : principales initiatives et organisations

Normes / organisations	Champ d'action	Pertinence canadienne
SCC mirror committees	Mécanismes de participation canadienne aux normes internationales (ex. ISO/IEC JTC 3 Technologies quantiques)	Permet aux entreprises canadiennes d'influencer et de demeurer alignées à l'échelle mondiale.
Cyber Centre / Government of Canada roadmap for post-quantum cryptography (CCCS)	Échéanciers nationaux de réponse au risque quantique (migration cryptographique).	Politiques et échéanciers canadiens directement applicables aux secteurs public et privé.
Canadian Forum for Digital Infrastructure Resilience (CFDIR)	Comment préparer la transition des systèmes numériques vers des technologies cryptographiques résistantes au quantique.	Techniques directement applicables pour accélérer la migration post-quantique à l'échelle de l'entreprise.
ITU-T Y.3800 (QKD networks)	Norme sur les communications quantiques (réseaux QKD)	Norme internationale ayant un impact sur les infrastructures canadiennes de communications et de cryptographie.

5.2.8

Advanced Cryptographic Concepts

Ce guide ne cherche pas à remplacer la littérature technique en cryptographie, mais la section suivante apporte des éclairages ciblés pour les lecteurs souhaitant aller plus loin.

Génération aléatoire

Depuis plusieurs années, des générateurs quantiques de nombres aléatoires sont disponibles sur le marché et sont recommandés pour toute application cryptographique nécessitant de l'aléa, comme le chiffrement ou les signatures numériques. À la différence des générateurs pseudo-aléatoires logiciels, ces dispositifs produisent un aléa réellement imprévisible, renforçant nettement la sécurité et la qualité de la cryptographie utilisée.

Sécurité computationnelle

Tous les systèmes de chiffrement à clé publique, tout comme les systèmes symétriques tels qu'AES, partagent une faiblesse commune : à tout moment, une attaque fondamentale peut être découverte, rendant déchiffrables tous les messages protégés par ce système. C'est essentiellement ce qui s'est produit avec l'algorithme de Shor; heureusement, les ordinateurs quantiques n'existaient pas encore lors de sa publication. Cela souligne l'importance de la prudence dans l'utilisation de ces systèmes de chiffrement.

Chiffrement à clé publique à deux clés

Pour les données hautement sensibles, il peut être judicieux de recourir à deux systèmes de chiffrement à clé publique pour l'échange des clés symétriques. Les clés restent alors protégées tant qu'au moins un des deux systèmes demeure sûr. En contrepartie, les messages d'encapsulation de clés (KEM) sont deux fois plus volumineux. (Il est très peu probable que CRYSTALS-KYBER et HQC soient compromis en même temps.)

5.3 Suppléments à ce guide

Si ce guide vous a été utile, les suppléments et guides compagnons suivants, actuellement en développement, pourraient vous intéresser.

- 1 Unités de travail, risques et indicateurs d'avancement de la migration vers la cryptographie post-quantique
- 2 Modèle de maturité des capacités quantiques et gabarits d'évaluation
- 3 Gabarit d'évaluation du risque quantique
- 4 Gabarit de rapport exécutif pour le suivi de la préparation quantique
- 5 Guide d'identification des cas d'usage quantiques et d'évaluation de leur faisabilité

5.5

Références et apprentissage continu

Source et lien	Vue d'ensemble du contenu
Perspectives stratégiques et sectorielles	
World Economic Forum: Quantum Technologies: Key Strategies and Opportunities for Financial Services Leaders”	Analyse comment les secteurs financiers peuvent exploiter l’innovation quantique de façon responsable, en maîtrisant les risques, la conformité et la confiance.
WEF Quantum Industry Initiative	Analyse comment l’informatique quantique peut être exploitée dans d’autres secteurs
Positionnement du Canada en matière de quantique	
Quantum Computing & Quantum Technology Initiatives in Canada	Historique de l’écosystème canadien de l’informatique quantique et analyse du positionnement national (datant de 2024, mais toujours très pertinent).
National Quantum Strategy roadmap: Quantum computing	La Stratégie nationale quantique du gouvernement du Canada (SNQ)
Natural Sciences and Engineering Research Council of Canada - Impact Analysis - Quantum Edition	Un regard sur les talents, la recherche et les innovations qui font du Canada un leader mondial en recherche quantique : milieu académique, industrie, science quantique, cybersécurité et systèmes de communication de nouvelle génération.
Quantum industries Canada	Industrie quantique Canada (QIC) est le consortium canadien dirigé par l’industrie dont la mission est de transformer les capacités et atouts quantiques du Canada en succès commerciaux mondiaux et en prospérité nationale.
Technologies quantiques et paysage de marché	
The Quantum Insider – “Top Quantum Computing Companies (2025)”	Dresse le profil des principales entreprises et jeunes pousses quantiques à l’échelle mondiale, incluant des acteurs canadiens de premier plan.
The Quantum Index	Une base de données mondiale recensant les startups quantiques, les investisseurs, les pôles de recherche et les partenariats au sein de l’écosystème émergent.
Risque quantique et cybersécurité	
An Interview with a Canadian Cryptography Pioneer	Souligne le leadership du Canada en recherche cryptographique et le caractère stratégique de la préparation post-quantique.
Best Practices for Quantum Readiness	Le Quantum Readiness Working Group (QRWG) du Forum canadien pour la résilience des infrastructures numériques (CFDIR), présente des meilleures pratiques en matière de préparation quantique et de migration vers la cryptographie post-quantique.
Quantum-readiness for the financial system: a roadmap	Un panorama de la cryptographie et des étapes concrètes d’alignement mondial des institutions bancaires, publié par la Banque des règlements internationaux.
Site Web de Kirq	Kirq est un banc d’essai en communication quantique qui combine les technologies quantiques et classiques dans des conditions réelles.
Global Risk Institute – “A Methodology for Quantum Risk Assessment”	Propose un cadre structuré d’évaluation des risques quantiques pour les institutions financières, centré sur la cryptoagilité et l’obligation fiduciaire.
Post Quantum Cryptography (PQC) Building Cryptographic Agility in the Financial Sector	Rédigé par le groupe de travail Post Quantum Cryptography du FS-ISAC, ce document détaille la cryptoagilité et propose des lignes directrices concrètes pour la mettre en œuvre.
Post-Quantum – “Practical Steps to Quantum Readiness”	Expose des stratégies concrètes de migration et de résilience pour préparer les organisations à la cryptographie post-quantique.

Leaders d'opinion qui enrichissent cet ouvrage.

Ce guide s'est construit grâce à la vision et à l'engagement de leaders conscients de l'urgence de préparer les organisations à l'ère quantique. Leurs apports ont été essentiels à la clarté, à la crédibilité et à la portée de cet ouvrage.



Claude Crépeau

Professeur au Département de génie logiciel et des technologies de l'information, École de technologie supérieure (ÉTS Montréal)

« Ce guide est une lecture essentielle pour quiconque s'intéresse à la sécurisation des transactions. D'une grande rigueur scientifique, il fait le lien entre le milieu académique et le monde financier. »



Marc Frappier, Ph.D., professeur

Titulaire de la chaire de recherche en cybersécurité post-quantique et directeur scientifique du Centre d'expertise en cybersécurité Intact à l'Université de Sherbrooke

« La préparation de la résistance aux attaques quantiques est un objectif stratégique à traiter dès maintenant. Ce guide permet aux dirigeants et aux conseils d'administration d'amorcer la planification de la transition vers la cryptographie post-quantique, une transformation majeure nécessitant une coordination étroite, la cryptographie étant au cœur de tout actif TI. »



Joni Brennan

Présidente, Conseil canadien de l'identification et de l'authentification numériques (DIACC).

« Comment quantique arrive à point nommé. Il clarifie les enjeux de la confiance numérique et de la vérification de l'identité à l'ère quantique, et trace une voie claire pour préserver la confiance des Canadiens. »



Christian Sarra-Bournet, PhD

Directeur Exécutif de l'Institut quantique de l'Université de Sherbrooke

« Je soutiens cette initiative, car les décideurs et dirigeants des grandes organisations doivent agir sans délai : l'inaction face aux menaces cryptographiques quantiques mettrait en péril l'intégrité de nos infrastructures critiques et ferait perdre une occasion stratégique de différenciation concurrentielle. »



Anne-Marie Hubert

Chercheur associée principal au CIRANO, Présidente du chapitre canadien de la Human Technology Foundation

« Le moment est venu de rejoindre un écosystème où gouvernements, investisseurs, scientifiques et entreprises unissent leurs forces pour capitaliser sur le leadership canadien, relever des défis majeurs et générer un rendement tangible pour les entreprises et une croissance durable pour les Canadiens. Une occasion à saisir. »



Charles Morgan

Membre du conseil consultatif (ancien président) de l'International Technology Law Association (ITechLaw), membre du conseil d'administration du chapitre canadien de la Human Technology Foundation

« L'informatique quantique constitue une technologie de rupture de nouvelle génération, susceptible de transformer en profondeur les organisations. Ce guide clarifie les facteurs essentiels que les conseils d'administration doivent considérer pour encadrer les risques et les opportunités liés au quantique. »



Suzanne Gouin

Présidente du conseil de gestion de l'Agence du revenu du Canada et administratrice de la Banque Laurentienne et de Polykar

« En tant que conseils d'administration, il est essentiel de reconnaître que l'informatique quantique transformera bientôt notre relation à la technologie. Cet ouvrage agit comme un signal d'alarme pour aider les conseils à comprendre les enjeux, la technologie et les échéanciers, et à se préparer à relever ce défi émergent tout en saisissant de nouvelles occasions. »



Bernard Duval

Présidente directeur-général du Numana, le commanditaire stratégique de Kirq - "le banc d'essai pour les communications sécurisées post-quantiques"

« Comment quantique aide les dirigeants à comprendre que les technologies quantiques sont avant tout un enjeu de gouvernance. Mais aussi une réalité actuelle, importante et urgente à considérer. Numana-Kirq transforme cette compréhension en capacité d'action. »

Réviseurs experts et conseillers

Assurer l'exactitude, la profondeur et la clarté

Ces personnes ont consacré temps, expertise et rétroaction critique pour revoir et améliorer le contenu. Leurs commentaires réfléchis ont renforcé la rigueur et la pertinence pratique du guide.

- **Martin Laforest:** Associé directeur, Quantacet, capital de risque et incubation quantique
- **Marin Ivezić:** PDG, Applied Quantum, chercheur et auteur en risques des technologies émergentes*
- **Bruno Couillard:** Crypto4A, PDG, leader en technologies de cryptographie quantique
- **Kit Dalaroy:** Président, Dalaroy Conseil, conseiller stratégique en croissance
- **Nicolas Tran:** Expert en risque opérationnel des services financiers
- **Alexis Arévalo:** Perspective exécutive sur les synergies quantique-bancaire

Rédaction et production

Les artisans derrière les mots

Mes sincères remerciements à **Valérie Boissonault**, dont la conviction précoce a été le catalyseur de cette initiative; à **Anne-Marie Hubert**, dont l'élan et le soutien l'ont portée; à **Christian Sarra-Bournet** pour son accompagnement réfléchi tout au long du parcours; et à **mon fils**, dont la clarté, les questions et les révisions ont permis de donner aux idées leur forme la plus aboutie.

Enfin, chapeau à **Laura Poulin**, pour son travail de design exceptionnel.

À propos de l'auteure



Louise Davey, fondatrice de LDIQ

Louise Davey est **architecte et leader en transformation organisationnelle**, forte de plus de **30 ans d'expérience** exécutive et de conseil. Elle aide des organisations publiques et privées à bâtir de nouvelles capacités, accroître leur agilité opérationnelle, renforcer leur gouvernance, maîtriser les risques et développer leur résilience grâce à l'adoption ciblée de technologies avancées.

Ancienne **CTO et COO, détentrice d'une maîtrise en physique** de McGill, **administratrice et leader de comité TI**, Louise traduit des concepts technologiques complexes (données, cybersécurité, IA, quantique) en résultats d'affaires mesurables, en leviers de résilience et d'agilité.

Ses travaux récents portent sur la conversion de la complexité du quantique et de la cryptographie en **information décisionnelle et actionnable**, en formulant les risques et opportunités post-quantiques en termes de **devoir fiduciaire, d'impact d'affaires et d'actions concrètes** pour mobiliser les dirigeants.





Merci de soutenir la diffusion de
ce guide en prenant part aux
échanges sur [LinkedIn](#).

Vous pouvez partager vos
commentaires directement ici :
ldiq.ca

