Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA sur la surveillance 05/2026

Informatique quantique

9 juillet 2026

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

1 Introduction

Fin 2025, l'Autorité fédérale de surveillance des marchés financiers (FINMA) a réalisé une enquête sur les opportunités et les risques liés à l'informatique quantique auprès de 60 établissements financiers suisses. Ces établissements sont conscients des cyberrisques liés aux ordinateurs quantiques cryptographiquement pertinents. La plupart d'entre eux ne disposent cependant pas d'une feuille de route claire ni d'une planification suffisante en vue de leur migration vers un chiffrement résistant aux attaques quantiques.

Dans le droit des marchés financiers, les exigences prudentielles fondées sur des principes et neutres sur le plan technologique visant à assurer une gouvernance et une gestion des risques efficaces s'appliquent aussi aux risques découlant de l'avènement d'ordinateurs quantiques performants. Conformément aux exigences internationales, la FINMA attend des assujettis qu'ils se penchent à temps sur ces risqueset adaptent leur gouvernance et leur gestion des risques en conséquence.

Forte de ses activités de surveillance, la FINMA considère qu'il serait opportun, pour de nombreux établissements, de faire évoluer leur gestion des risques de manière à garantir le respect des prescriptions en vigueur en matière de risques opérationnels et de résilience.

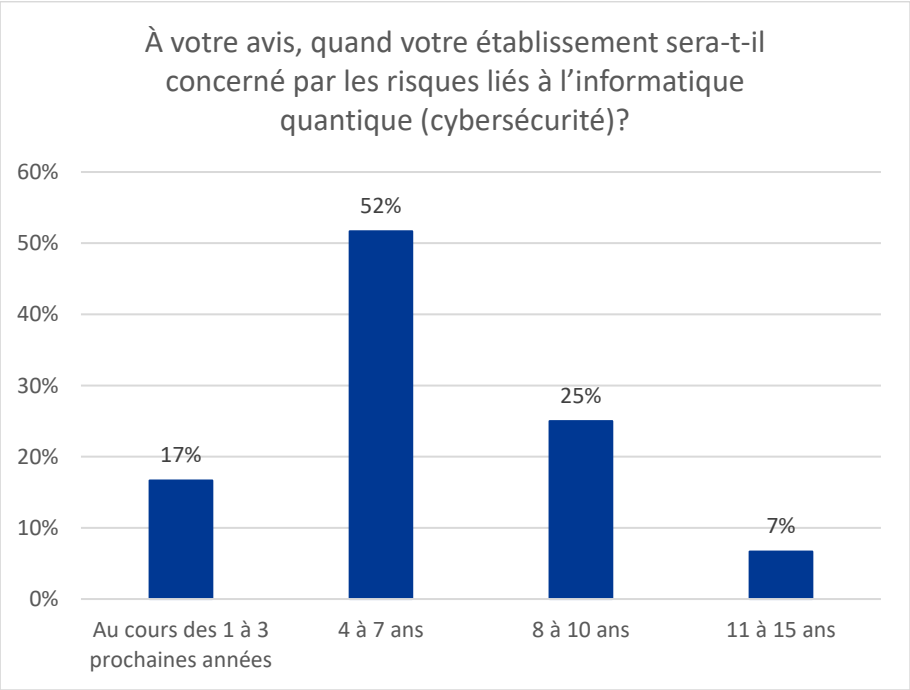
2 Résultats de l'enquête

De novembre 2025 à janvier 2026, la FINMA a interrogé au total 60 entités autorisées (banques, entreprises d'assurance, gestionnaires de fortune collective et infrastructures des marchés financiers) sur les opportunités et les risques liés à l'informatique quantique. Les résultats de cette enquête montrent que les établissements financiers suisses sont généralement conscients des cyberrisques découlant des ordinateurs quantiques, en particulier de la menace potentielle qu'ils représentent pour la sécurité des technologies de chiffrement. La plupart des établissements n'en sont toutefois qu'aux prémices d'une transition vers un chiffrement résistant aux attaques quantiques.

Les établissements ont conscience des cyberrisques liés à l'informatique quantique

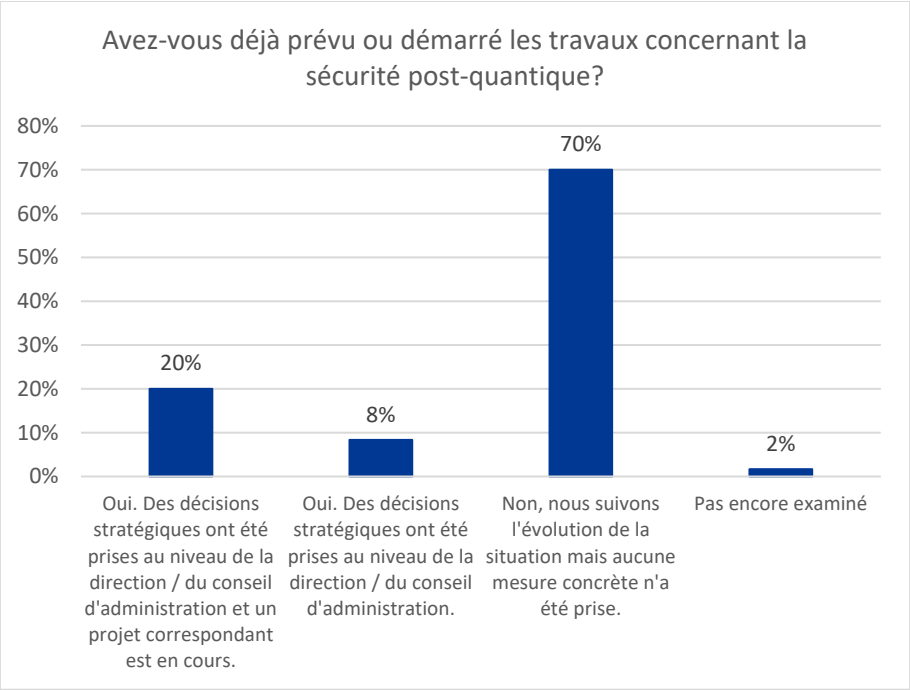
Environ deux tiers des établissements interrogés s'attendent à être directement concernés par les cyberrisques liés à l'informatique quantique dans les sept ans au plus. Ils sont environ deux tiers également à estimer que dans dix ans au plus tard, il ne faudra pas plus de 24 heures à un ordinateur

quantique pour casser un chiffrement RSA à 2048 bits. Pour les établissements interrogés, les principaux risques découlant des ordinateurs quantiques concernent donc la sécurité des données. D'autres risques importants sont également soulignés: une migration incomplète vers un chiffrement résistant aux attaques quantiques, un manque de savoir-faire, des attaques du type «collecter aujourd'hui, décrypter demain» (*harvest now, decrypt later*, HNDL) ainsi que l'interopérabilité avec les systèmes hérités.



Peu d'établissements ont une feuille de route en vue de l'adoption d'un chiffrement résistant aux attaques quantiques

72 % des établissements interrogés indiquent soit n'avoir pas encore planifié de mesures en vue de l'adoption d'un chiffrement résistant aux attaques quantiques, soit n'avoir pas commencé à mettre en œuvre de telles mesures. Les autres, autrement dit 28 %, ont déjà pris une décision stratégique en la matière et 20 % ont un projet en cours.



Seuls 8 % des établissements interrogés disposent d'une feuille de route concrète en matière de chiffrement résistant aux attaques quantiques. Selon ces feuilles de route, leurs données et processus critiques seront protégés contre les risques quantiques d'ici quatre à cinq ans. La moitié environ des établissements interrogés prévoient d'établir une feuille de route d'ici un à trois ans, tandis que 43 % n'ont encore rien décidé à ce sujet.

La cryptoagilité, l'inventaire et les partenaires externes sont des facteurs importants

Les établissements interrogés s'accordent à souligner l'importance de deux facteurs aux fins de la transition vers une cryptographie post-quantique (CPQ): d'une part la cryptoagilité – c'est-à-dire la capacité des systèmes informatiques de changer d'algorithmes de chiffrement rapidement et en toute flexibilité –, qui est qualifiée d'importante ou très importante (73 %); d'autre part l'établissement d'un inventaire des processus cryptographiques utilisés, qui est considéré comme présentant une valeur ajoutée élevée ou très élevée (76 %). La majorité des établissements n'ont pas encore décidé s'ils feront appel aux services de tiers pour réaliser leur migration vers la CPQ. Les partenaires externes et les éditeurs de logiciels revêtent cependant dans tous les cas une importance centrale, car les cyberrisques sont également pertinents à leur niveau et à celui des interfaces. Parmi les établissements interrogés, 60 % ont déjà pris contact avec des éditeurs de logiciels ou prévoient de le faire.

Deux tiers des établissements estiment qu'ils se serviront de l'informatique quantique dans leur entreprise dans huit ans au plus tôt

Pour les établissements interrogés, la plus grande valeur métier des ordinateurs quantiques réside dans l'analyse des risques et des portefeuilles, dans la surveillance des transactions, dans le *trading* algorithmique ainsi que dans la génération de nombres aléatoires de meilleure qualité. Ils sont nombreux toutefois à considérer que le niveau de maturité actuel de la plupart des applications propres à leur branche ne dépasse pas encore le stade de la recherche ou du développement initial. Un tiers de ceux qui ont déjà réfléchi à l'utilisation d'ordinateurs quantiques dans leur entreprise considèrent que les conditions préalables les plus importantes pour cette utilisation sont l'accès au savoir-faire et à une main-d'œuvre spécialisée, ainsi que la disponibilité d'un matériel informatique stable. Près des deux tiers des établissements interrogés estiment qu'ils ne se serviront eux-mêmes d'applications quantiques que dans huit ans au plus tôt.

Conclusions de l'enquête

De manière générale, l'enquête montre que de nombreux assujettis sont conscients des futurs risques liés à l'informatique quantique, mais que seuls quelques-uns prennent des mesures concrètes visant à contrer ces risques. Dans ce contexte, la FINMA appelle l'attention sur le fait que la recherche se traduit par de constants progrès techniques, que les projets de migration vers la CPQ sont des projets de longue haleine et qu'il n'est pas possible de dire avec certitude dans combien de temps des ordinateurs quantiques cryptographiquement pertinents seront disponibles.

3 Recommandations

Les recommandations qui suivent se fondent sur les activités de surveillance de la FINMA. Elles sont portées ici à la connaissance des assujettis concernés, qui sont invités à en tenir compte dans leur gestion interne des risques.

Les recommandations se limitent à la migration vers des algorithmes résistants aux attaques quantiques[1] et ne portent pas sur l'utilisation de la distribution quantique de clés (*quantum key distribution*, QKD) ni sur les questions que les applications d'informatique quantique peuvent soulever.

[1] ML-EM, NIST, FIPS 203, https://csrc.nist.gov/pubs/fips/203/final; ML-DAS, NIST, FIPS 204, https://csrc.nist.gov/pubs/fips/204/final; SLH-DAS, NIST, FIPS 205, https://csrc.nist.gov/pubs/fips/205/final

3.1 Stratégie et feuille de route

La FINMA recommande que les travaux de migration vers un chiffrement résistant aux attaques quantiques reposent sur une stratégie adoptée par l'organe responsable de la haute direction, sur la base de laquelle un plan de mise en œuvre comprenant des jalons et des priorités (feuille de route CPQ) doit être élaboré. Il est conseillé en particulier de fixer des dates butoirs pour l'achèvement de la migration ainsi que pour la migration des processus d'entreprise critiques vers une cryptographie résistante aux attaques quantiques. La FINMA invite à élaborer la feuille de route CPQ pour le milieu de 2027 au plus tard.

La stratégie CPQ peut s'inscrire dans le cadre d'une stratégie existante (p. ex. en matière de cyberrisques).

3.2 Analyse des risques et inventaire

Du point de vue de la FINMA, la première étape du passage à un chiffrement résistant aux attaques quantiques doit consister en une analyse des risques portant, d'une part, sur les algorithmes cryptographiques utilisés et, d'autre part, sur les données critiques devant être protégées à long terme.

La FINMA incite par conséquent à analyser en détail tous les processus métier sous l'angle des technologies de chiffrement, de signature et d'authentification utilisées. Elle considère que cette analyse doit couvrir tous les systèmes relevant des technologies de l'information et de la communication (systèmes TIC) ainsi que toutes les applications, les infrastructures et les technologies de conception nouvelle – telles que le registre électronique distribué (cf. art. 973*d* al. 2 ch. 2 du code des obligations [RS 220]) –, peu importe qu'ils soient exploités en interne, externalisés ou utilisés en tant que service.

Pour la FINMA, cette analyse des processus opérationnels doit déboucher sur l'établissement d'un inventaire complet des processus cryptographiques utilisés. En font partie le chiffrement des données lors de leur transmission (protocoles VPN, TLS, HTTPS, etc.) et celui des données stockées, de même que l'utilisation de signatures numériques, la gestion des clés ainsi que les mécanismes d'authentification utilisés. Un tel inventaire permet en outre d'identifier les algorithmes vulnérables aux attaques quantiques[2] et devant donc être remplacés. Pour les systèmes utilisant de tels algorithmes, un plan de migration adapté au risque qu'ils constituent doit être établi d'après la FINMA. Enfin, tenir à jour cet inventaire cryptographique de manière qu'il reflète constamment la situation effective contribue à l'efficacité de tout le dispositif.

[2] Par exemple RSA, ECDSA, EdDSA, DH, EC-DH

3.3 Données critiques

Il est également recommandé, dans le cadre de l'analyse des risques, de recenser et d'analyser les besoins de protection des données critiques. Il convient en particulier d'examiner s'il est nécessaire de fournir des garanties de sécurité à long terme en matière de confidentialité et d'intégrité des données, ou encore de garantir le principe de non-répudiation, par exemple pour les signatures électroniques. La FINMA recommande de prendre également en compte le risque d'attaques de type «collecter aujourd'hui, décrypter demain», autrement dit le risque que des données chiffrées soient dérobées aujourd'hui dans l'intention de les décrypter ultérieurement à l'aide d'ordinateurs quantiques performants. Les données devant être protégées à long terme doivent donc être traitées en priorité et sécurisées en conséquence à l'aide d'algorithmes CPQ.

Étant donné que l'on ne dispose pas encore d'expérience à long terme en matière d'algorithmes CPQ, plusieurs organisations[3] recommandent d'opter, à court et à moyen terme, pour des solutions hybrides plutôt que pour des algorithmes CPQ purs. Cette approche consiste à combiner un algorithme traditionnel et un algorithme CPQ, ce qui renforce la sécurité et la garantit même si l'un des deux algorithmes s'avère vulnérable. Le chiffrement hybride est souvent cité pour protéger les données critiques en particulier contre le risque d'attaques de type «collecter aujourd'hui, décrypter demain». Il implique cependant une complexité accrue, ce qui comporte des risques liés à sa mise en œuvre. Enfin, l'analyse interne des risques peut également mettre en évidence l'opportunité de recourir à des solutions hybrides également pour la migration des systèmes.

3.4 Cryptoagilité

Il faut s'attendre à l'avenir également à ce que des algorithmes (CPQ) considérés actuellement comme sûrs doivent être remplacés. Certains algorithmes CPQ pourraient en effet – contre toute attente – ne pas faire leurs preuves.

La cryptoagilité désigne la capacité d'un système TIC ou d'une application à changer d'algorithmes cryptographiques en toute flexibilité. Elle ne se limite pas à la migration vers des algorithmes CPQ, mais concerne l'ensemble des algorithmes utilisés. Il est donc recommandé de faire de la cryptoagilité une propriété dont tous les systèmes TIC ainsi que toutes les applications à acquérir ou à développer doivent être dotés. Cela garantit qu'ils puissent changer d'algorithmes de chiffrement de manière flexible et sans modifications profondes de leur architecture logicielle.

[3] «Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptograph. A joint statement from partners from 21 European states», 2025, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3

3.5 Prestataires externes

Que ce soit lors de l'externalisation de fonctions ou en relation avec des interfaces de communication externes, la migration CPQ implique généralement des dépendances à l'égard de prestataires externes. Ces prestataires doivent eux aussi implémenter, dans leurs systèmes, une cryptographie résistante aux attaques quantiques, afin de continuer à garantir la sécurité requise lorsque des ordinateurs quantiques performants seront disponibles. Pour assurer une planification et une mise en œuvre de la migration appropriées et économiquement efficientes, il est dans la plupart des cas judicieux de l'inscrire dans des cycles de mises à jour réguliers. Cela requiert une planification à long terme en collaboration avec les prestataires externes pour tout ce qui concerne les nouvelles exigences.

La responsabilité des fonctions externalisées incombe dans tous les cas à l'établissement qui les externalise (cf. à ce sujet la circulaire FINMA 2018/3 «*Outsourcing*»). Les risques futurs – tels que ceux liés à des ordinateurs quantiques performants – peuvent, eux aussi, être anticipés et les mesures nécessaires définies contractuellement avec les prestataires externes dès aujourd'hui.

Enfin, il est recommandé de faire de la cryptoagilité[4] une condition de toute nouvelle relation d'externalisation concernant des logiciels ou des données, ou de l'intégrer rapidement dans les exigences des relations d'externalisation existantes.

4 Perspectives

Il n'existe pas encore d'ordinateurs quantiques cryptographiquement pertinents. Les progrès techniques ont toutefois gagné en dynamisme et leur développement est à prévoir dans les années à venir. Il est donc indispensable de rapidement mettre en place une gestion appropriée des cyberrisques liés à l'informatique quantique.

En prévision de l'émergence des risques découlant des ordinateurs quantiques, la FINMA invite à d'ores et déjà y réfléchir et agir pour les réduire – cela en raison notamment de la complexité de la migration vers des technologies de chiffrement résistantes aux attaques quantiques et du temps qu'elle nécessite, des interdépendances entre les prestataires et les établissements financiers et du risque déjà bien réel actuellement d'attaques de type «collecter aujourd'hui, décrypter demain».

[4] Capacité des systèmes informatiques à changer d'algorithmes de chiffrement de manière flexible et sans modifications profondes de leur architecture logicielle

La FINMA entend suivre activement les développements en cours dans le domaine de l’informatique quantique et renforcer la place occupée par cette thématique dans ses activités de surveillance courantes.