DataNavigator

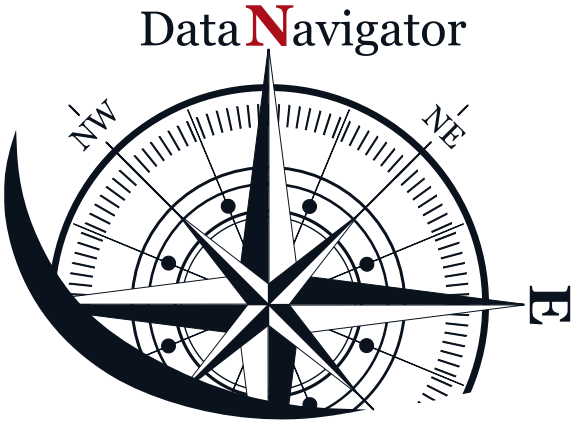
www.datanavigator.de | ISSN 2702-1904

Quantencomputer – Überblick über Status und Handlungsbedarf

Carsten Striebich

#32 | November 2025

EUROGROUP CONSULTING



Quantencomputer und deren schneller technischer Fortschritt werden aktuell stark beachtet. So hat die UNO 2025 zum Jahr der Quantentechnologie ausgerufen. Auch Bundeskanzler Friedrich Merz hat nach der Kabinettsklausur in Potsdam im September Künstliche Intelligenz (KI) und Quantencomputing als wesentliche Zukunftstechnologien benannt, die die Bundesregierung fördern und unterstützen wird.

Doch wie weit sind Quantencomputer wirklich? Müssen sich Banken, Versicherungen und sonstige Finanzdienstleistungsunternehmen bereits heute darauf vorbereiten? Diese Frage ist eindeutig mit ‚Ja' zu beantworten.

Während einige wenige große Institute sich schon seit längerer Zeit mit Quantencomputern, Quantensoftware und Quantenkryptographie beschäftigen, haben die meisten Banken, Versicherungen und sonstige Finanzdienstleistungsunternehmen aktuell noch keine relevanten Aktivitäten zur Vorbereitung auf die notwendige Transformation gestartet. Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) ruft aber dazu auf, sich schon heute intensiv mit den Auswirkungen zu beschäftigen. Sie sieht durch die Einführung hochleistungsfähiger Quantencomputer große Risiken auf Banken und andere Finanzkonzerne zukommen. So warnte etwa BaFin-Präsident Mark Branson: ‚Quantencomputer werden etablierte Verschlüsselungsverfahren überwinden können'.[1]

Weshalb das so ist, welche Risiken und Chancen mit Quantencomputern verbunden sind und welcher dringende Handlungsbedarf konkret besteht, zeigen wir in diesem Artikel.

Quantencomputer – eine völlig andere Technologie

Ein Quantencomputer ist ein neuer Computertyp, der auf den Prinzipien der Quantenmechanik basiert, also der Physik, die das Verhalten kleinster Teilchen wie Atome und Elektronen beschreibt. Während herkömmliche Computer mit Bits rechnen, die nur den Zustand 0 oder 1annehmen können, arbeiten Quantencomputer mit Quantenbits (Qubits). Qubits können auch in Überlagerungszuständen rechnen, also auch Zustände zwischen 0 und 1 annehmen. Sie

[1] Vgl. Handelsblatt vom 02.07.2025.

nutzen physikalische Effekte der Quantenmechanik wie Superposition und Verschränkung, um Rechnungen auf eine schnellere Art zu skalieren als klassische Rechner.

Quantencomputer sind deshalb für ausgewählte Anwendungsfälle nicht nur deutlich schneller als herkömmliche Computer, sondern auch die erste wirkliche grundlegende technologische Änderung in der Hardware seit der Entwicklung von Mikrochips in den 60er bzw. 70er Jahren des 20. Jahrhunderts mit entsprechenden Herausforderungen für die IT-Abteilungen von Banken, Versicherungen und sonstigen Finanzdienstleistungsinstituten. Tabelle 1 stellt die wesentlichen Unterschiede gegenüber.

Klassischer Computer	Quantencomputer
Nutzt Bits: 0 oder 1	Nutzt Qubits: 0 und 1 gleichzeitig (Superposition)
Rechnet Schritt für Schritt	Kann viele Zustände parallel berechnen
Stabil	Sehr empfindlich gegenüber Störungen
Gut für Alltagsaufgaben	Besonders stark bei bestimmten Spezialproblemen

Tabelle 1 – Vergleich klassische Computer mit Quantencomputern

Anders als bei herkömmlichen Computern, die alle auf den gleichen Grundprinzipien aufgebaut sind, gibt es bei Quantencomputern völlig verschiedene technische Lösungen bzw. Hardware-Ansätze, beispielsweise supraleitende Qubits, Ionenfallen, Silizium-Spin-Qubits oder Photonen. Jeder dieser Ansätze hat eigene Vor- und Nachteile bei der Skalierbarkeit, Fehleranfälligkeit und Steuerbarkeit.

Für ausgewählte Anwendungsfälle sind Quantencomputer milliardenfach schneller als herkömmliche Rechner. Während beispielsweise das Entschlüsseln einer aktuell üblichen Verschlüsselung mit einem herkömmlichen Rechner 1 Milliarde Jahre dauern würde, kann es ein Quantencomputer schaffen, den Code in ca. 100 Sekunden zu entschlüsseln. Dies resultiert daher, dass die Rechenleistung von Quantencomputern nicht linear ist, sondern sich mit jedem zusätzlichen Qubit verdoppelt. Mit zwei Qubits hätte man vier, mit drei schon acht Kombinationsmöglichkeiten. Entscheidend ist jedoch nicht nur die Quantität der Qubits, sondern vor allem deren Qualität, die Verschränkungen der Qubits und die Kohärenzzeit, die das Quantensystem stabil bleibt, um zu rechnen.

Quantencomputer werden in wenigen Jahren in der Breite für konkrete Use Cases anwendungsreif sein. Heute sind bereits sogenannte Noisy Intermediate-Scale Quantum (NISQ)-Quantencomputer verfügbar. Diese sind insbesondere nützlich für Forschung und Pilotanwendungen, aber noch fehleranfällig. Die Entwicklung schreitet allerdings schnell voran. In den Jahren 2024 und 2025 haben verschiedene Unternehmen wichtige Verbesserungen bei Fehlerraten, Gate-Fidelity oder neuen Qubit-Plattformen gemeldet.

Eine Vielzahl an etablierten Technologiekonzernen aber auch neue Unternehmen arbeiten daran, anwendungsreife Quantencomputer herzustellen. IBM, Google, IonQ oder IQM sind einige der Unternehmen. Viele bieten heute schon Rechenzeit auf Quantencomputer für Prototypen an und verfügen über eine klare Roadmap. Abbildung 1 gibt einen Überblick über die wesentlichen Hersteller und deren Entwicklungsansätze.

IBM	Setzt auf supraleitende Quantenprozessoren und hat eine langfristige Roadmap. Bis 2029 plant IBM, ein System mit 200 logischen Qubits (fehlerkorrigiert; „error correction“) bereitzustellen, 2033 sollen es bis zu 2.000 logische Qubits werden. Aktuell wird an Roadmap-Zwischenzielen gearbeitet, wie einem Rechner mit 156 Qubits und einer Reduktion der Fehler („error mitigation“).
Google	Demonstrierte 2019 Quantenvorsprung und entwickelt weiter supraleitende Chips. Im Dezember 2024 stellte Google den „Willow“-Chip (~100 Qubits) vor, der deutlich bessere Fehlerbekämpfung zeigte und in einer Benchmark-Aufgabe einen klassischen Supercomputer um ein Vielfaches übertraf. Google arbeitet auf eine fehlerkorrigierte Großmaschine bis etwa 2029 hin und investiert über die „Quantum AI“ und Zukauf (z.B. MIT-Start-up Atlantic Quantum) in skalierbare Hardware.
IonQ	Führend bei Ionenfallen-Systemen. Die Roadmap sieht 2027 einen Monolith-Chip mit 10.000 Qubits und 2028 ein Netzwerk aus zwei 10.000-Qubit-Chips (20.000 Qubits) vor. Bis 2030 sollen durch Vernetzung ca. 2 Millionen physische Qubits (40.000–80.000 logische Qubits) erreicht werden. IonQ setzt auf modulare, photonen-vernetzte Architektur und plant so, als erster breite Quanten-Netzwerke zu realisieren.
IQM	Spezialisiert sich auf supraleitende Qubits und entwickelt Hardware (Quantenprozessoren), Software (Hardware-Software-Stack) und Integration in Recheninfrastrukturen (z. B. wie Quanten-HPC Hybride Systeme). Das Unternehmen setzt auf „Full-Stack“ Lösungen. Bereitstellung geplant in 2026 (150-Qubit) und 2027 (300-Qubit) mit Schwerpunkt auf Fehlerkorrektur (QEC). Beteiligung an einem großen europäischen Forschungsprojekt mit Ziel eines 1.000-Qubit supraleitenden Systems.
Weitere Hersteller: Rigetti, Quantinuum, Microsoft	Rigetti (USA) kündigte an, als nächsten Schritt von 36 auf mehr als 100 Supraleiter-Qubits zu kommen. Quantinuum (UK/USA) plant mit dem Ionensystem „Apollo“ und neuen Algorithmen eine universelle, fehlerkorrigierte Maschine bis ~2030. Microsoft erforscht topologische Qubits (Majorana-Qubits – 2023 erster experimenteller Nachweis) und strebt langfristig robuste Quantenprozessoren an.

Abbildung 1 – Wesentliche Hersteller von Quantencomputern und deren Entwicklungsschritte

Viele Firmen kommunizieren auch konkrete Roadmaps mit Zwischensystemen, Skalierungsschritten und Zieljahren wie beispielsweise 2029 für anwendungsreife, überlegene Systeme, wie in der Roadmap von IBM in Abbildung 2 dargestellt.

Auch wenn der genaue Zeitpunkt unscharf bleibt, stimmen Experten aufgrund der Vielzahl an Anbietern und der Bündelung der Ankündigungen darin überein, dass leistungsstarke, fehlerkorrigierte alltagstaugliche Rechner, welche die Rechenleistung herkömmlicher Rechner deutlich übertreffen werden, zum Jahr 2029 bzw. 2030 (»Q-Day«) möglich sind.

Wegen dieser – trotz Unsicherheit – vergleichbar kurzen Zeitspanne empfehlen Aufsichtsbehörden wie die Bafin oder das Bundesamt für Sicherheit in der Informationstechnik (BSI) allerdings, bereits heute migrations- und risikobasierte Vorsorge zu treffen.

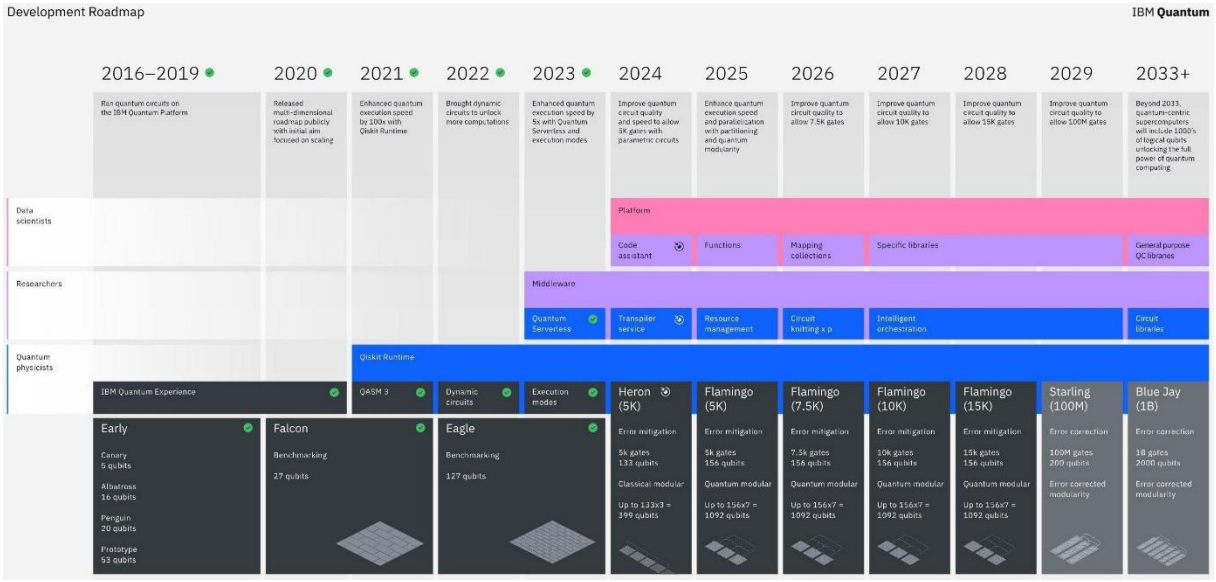


Abbildung 2 – Roadmap von IBM zur Entwicklung eines Quantencomputers (Quelle: IBM Quantum)

Einsatzmöglichkeiten von Quantencomputern

Wie bei jeder neuen Technologie stellt sich natürlich die Frage, welche Auswirkungen diese auf verschiedene Branchen und Institute haben wird. Es gilt daher abzuschätzen, für welche Anwendungsfälle Banken, Versicherungen und sonstige Finanzdienstleistungsunternehmen Quantencomputer einsetzen können. Quantencomputer sind, aufgrund ihrer anderen technischen Basis, nicht für alle Anwendungsfälle gleich gut geeignet. Für manche Anwendungen sind sie allerdings milliardenfach schneller als herkömmliche Rechner.

Entschlüsselung verschlüsselter Daten: Post-Quanten-Kryptographie (PQC)

Für die Verschlüsselung von Daten beginnt mit Quantencomputern eine neue Ära. Kryptographische Verfahren, wie die weit verbreitete RSA-Verschlüsselung, werden durch Quantencomputer angreifbar. Deshalb ist es erforderlich, heutige Verschlüsselungen quantensicher zu gestalten. Hierzu sind Post-Quanten-Kryptographieverfahren einzuführen. Post-Quanten-Kryptographie (PQC) bezeichnet kryptographische Verfahren, die so entworfen sind, dass sie auch gegen Angreifer mit leistungsfähigen Quantencomputern sicher bleiben. Standardisierungs-Gremien, insbesondere das National Institute of Standards and Technology (NIST) aber auch das Bundesamt für Sicherheit in der Informationstechnik (BSI), haben Algorithmen ausgewählt. Die NIST beispielsweise veröffentlicht seit 2023/2024 hierzu konkrete Federal Information Processing Standards (FIPS).

Besonders kritisch wird gesehen, dass heute bereits verschlüsselte Daten abgezogen und gespeichert werden können, die dann später durch Quantencomputer entschlüsselt werden können (‚harvest now – decrypt later'). Deshalb empfiehlt die Bafin, bereits heute zeitnah auf sichere Post-Quanten-Kryptographieverfahren umzusteigen.

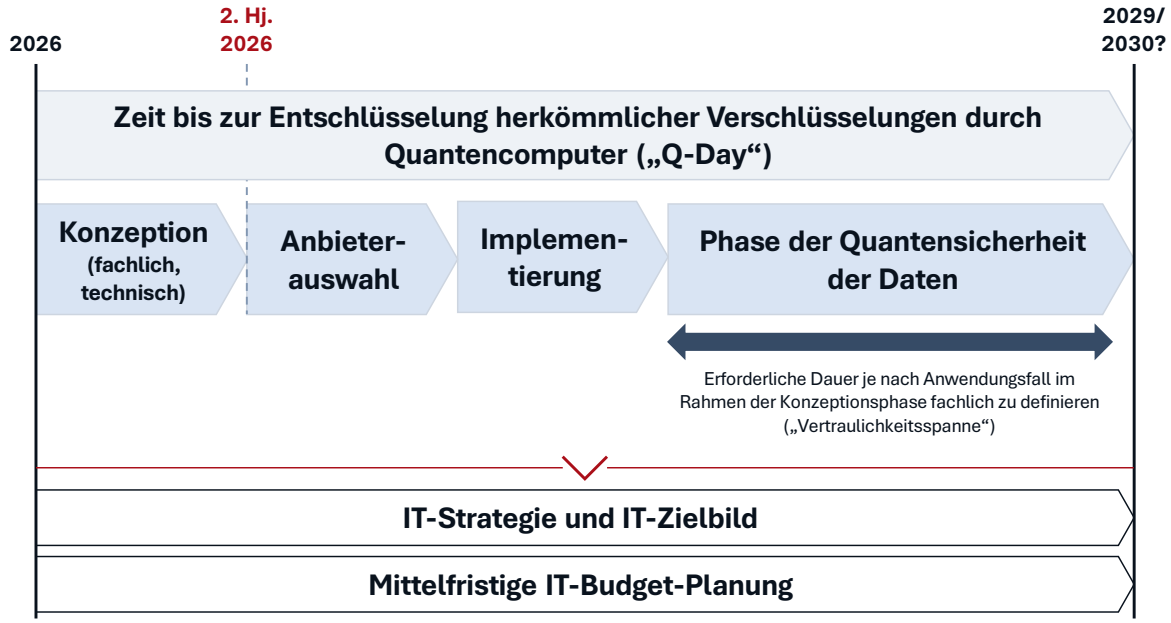


Abbildung 3 – Einführungsplanung für PQC-Verfahren

PQC-Algorithmen verlangen größere Schlüssel oder Signaturen als heute gebräuchliche Verschlüsselungsverfahren. Das wirkt sich auf Protokolle, Speicher und Netzwerkdurchsatz aus. Ebenso sind ausreichend leistungsfähige CPUs und Speicherbedarf erforderlich, Protokolle wie

VPNs müssen angepasst oder erweitert werden sowie Bibliotheken (OpenSSL, etc.) geprüft und ggf. aktualisiert werden.

Quantum Key Distribution (QKD)

Quanten-Kryptographie bezeichnet Verfahren, die Quanteneffekte nutzen, um Schlüssel für verschlüsselte Kommunikation physikalisch sicher zu übertragen. Der bekannteste Teilbereich ist die Quantum Key Distribution (QKD). Zwei Parteien erzeugen gemeinsam einen geheimen Schlüssel so, dass jede Abhöraktion physikalisch nachweisbar ist. Die eigentliche Übertragung der Daten erfolgt dabei über herkömmliche Verfahren. Dabei gibt es verschiedene Verfahren, beispielsweise diskrete-Variable-QKD (Photonen-Polarisation), kontinuierliche-Variable-QKD (Messung von Amplituden und Phasen) sowie fortgeschrittene Konzepte wie device-independent QKD oder satellitengestützte QKD.

Während grundsätzlich alle Daten quantensicher zu verschlüsseln sind, sind auf absehbare Zeit Quanten-Kryptographie-Netzwerke nur für besonders kritische und vertrauliche Daten erforderlich. Dies umfasst beispielsweise

- sichere Verbindungen zwischen Rechenzentren, besonders für hochsensitiven internen Verkehr (z.B. Clearing, Settlement),
- Absicherung von SWIFT/Interbank-Kommunikation und Marktinfrastruktur für eine langfristige Geheimhaltung für Zahlungs-/Clearing-Kommunikation und kritische Finanznachrichten,
- sichere Backups und Archivierung zum Schutz von besonders langfristig vertraulichen Daten (z. B. Vertragsarchive, Urkunden-Daten) und
- sichere Verbindungen für kritische Dienste oder CEO-Kommunikation durch hochwertige, physikalisch abgesicherte Kanäle für Management, Compliance-Kommunikation und Incident Response.

Während Banken, Versicherungen und sonstige Finanzdienstleistungsunternehmen schon heute aufgefordert sind, eigenständig auf sichere Post-Quanten-Kryptographieverfahren umzusteigen, besteht für die meisten Häuser aktuell noch kein Handlungsbedarf, QKD-Verfahren einzuführen. Allerdings wurden von zahlreichen Institutionen erste Initiativen und Pilotprojekte gestartet (z.B. DemoQuanDT, QuNET, EuroQCI). Mehrere europäische Banken wie die Bundesbank, die Banque de France oder HSBC beteiligen sich an diesen Initiativen bzw. führen derzeit Proof-of-Concept-Tests durch, um die Anwendbarkeit von QKD in verschiedenen Finanzszenarien zu evaluieren. Diese Tests konzentrieren sich auf die Integration von QKD in bestehende Infrastrukturen und die Bewertung der praktischen Umsetzbarkeit. Es ist deshalb davon auszugehen, dass es perspektivisch auch für die übrigen Finanzdienstleister erforderlich werden wird, ausgewählte, besonders schützenswerte Kommunikation auf QKD umzustellen. Folglich ist es notwendig, schon heute die Aktivitäten von zentralen Stellen und Wettbewerbern zu beobachten, um sich frühzeitig und bestmöglich auf kommende Anforderungen vorzubereiten und die Auswirkungen auf die eigene IT-Landschaft rechtzeitig abzuschätzen.

Quantenalgorithmen und Use Cases

Quantencomputer versprechen bei bestimmten Problemen (z.B. Monte-Carlo-Simulationen, kombinatorische Optimierung, lineare Algebra, Sampling/Schätzung) sehr deutliche

Performance-Vorteile, oft als quadratischer Speed-up, bzw. eine deutliche Verbesserung der Genauigkeit der Ergebnisse gegenüber klassischen Methoden. Aufgrund der deutlichen Überlegenheit der Ergebnisse ist es für Finanzdienstleistungsunternehmen ebenfalls zwingend erforderlich, rechtzeitig die Umstellung auf Quantenalgorithmen einzuleiten, um keine signifikanten Wettbewerbsnachteile zu erleiden. Sofern ein Finanzdienstleistungsunternehmen im Quantenzeitalter noch ‚klassische' Algorithmen beispielsweise zur Risikobewertung oder Fraud Detection nutzt, hat es einen signifikanten Wettbewerbsnachteil. Erste Proof-of-Concepts und Pilotprojekte sind bereits zu beobachten.

So hat die britische Großbank HSBC nach eigenen Angaben einen Durchbruch beim Einsatz von Quantencomputern im Anleihehandel erzielt. Es sei gelungen, die Vorhersagegenauigkeit für die Preissetzung im Handel um 34% zu verbessern. Da schon kleine Verbesserungen bei Preisprognosen Milliarden bewegen können, erkennt HSBC hier einen ‚Sputnik-Moment' für die Finanzbranche.[2] Als weitere mögliche Anwendungsfälle können genannt werden:

- Pricing / Risikobewertung durch Monte-Carlo-Simulationen
- Portfolio- und Asset-Allocation-Optimierung
- Handelsstrategie und Order-Execution (Market-Making, Liquidity)
- Kredit-Scoring, Kundensegmentierung und Fraud Detection
- Optimierung von Back-Office und Betriebsprozessen
- Versicherungsaktuarielle Modellierung und Reservierung

Experten gehen davon aus, dass ab dem Jahr 2028 erste, spezielle Anwendungsfälle praktischen Mehrwert liefern werden. Der Durchbruch in der Breite wird dann ab den Jahren 2029 bzw. 2030 erwartet.

Handlungsbedarf für Finanzdienstleister

Für Banken, Versicherungen und andere Finanzdienstleistungsunternehmen stellt sich damit die Frage, was nun konkret getan werden muss. Um sich auf die erforderliche Transformation hin zu Quantencomputern, Quantensoftware und Quantenkommunikation vorzubereiten, ergeben sich verschiedene Handlungsfelder.

Quantencomputer bzw. die Vorbereitung auf deren Auswirkungen sind ein strategisches Thema, das auf Vorstandsebene verankert werden muss. Aufgrund der großen geschäftspolitischen Auswirkungen muss es ‚von oben' in das Haus eingesteuert werden. Es sollte in Vorstandssitzungen regelmäßig über die laufenden Aktivitäten und deren Umsetzungsstand berichtet werden. Entsprechende Grundsatzentscheidungen sind auf Vorstandsebene herbeizuführen. Sofern bereits Initiativen gestartet wurden, sind ggf. laufende Einzelinitiativen in eine Gesamtstrategie zu integrieren.

Unterhalb der Vorstandsebene ist eine zentrale Stelle zu benennen, die die Transformation insgesamt koordiniert und verantwortet. Ebenfalls sind Technologie-, Markt- und Wettbewerberbeobachtung aufzusetzen sowie die zentrale Steuerung der Initiativen zu etablieren. So können die notwendigen Aktivitäten im Auftrag des Vorstands koordiniert und gesteuert werden. Es ist

[2] Vgl. Handelsblatt vom 25.09.2025.

zudem notwendig, einen Kommunikationsprozess zu beginnen und auch die Fachbereiche insgesamt auf das Thema Quantencomputer hin zu sensibilisieren. Auch Fachbereiche sind beispielsweise gefordert, bei der Identifikation und Umsetzung von Use Cases mitzuwirken.

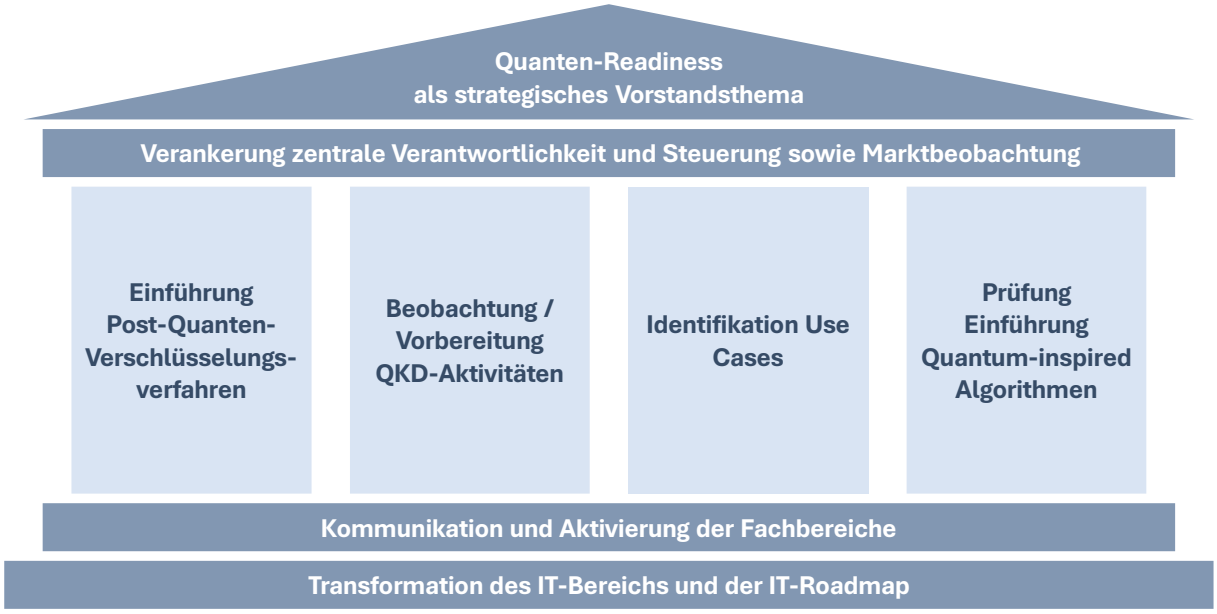


Abbildung 4 – Handlungsfelder für Finanzdienstleister zur Herstellung der Quanten-Readiness

Weiterhin sind die Auswirkungen von Post-Quanten-Kryptographie, Quantencomputern, Quantenalgorithmen und Quanten-Kryptographie auf das langfristige IT-Zielbild, die IT-Roadmap und die mittelfristige Budgetplanung abzuschätzen. Ebenfalls werden sich die Anforderungen an die eigene IT-Abteilung verändern. Quantencomputer basieren auf technisch vollkommen anderen Lösungen als herkömmliche Computer und Quantenalgorithmen unterscheiden sich fundamental von heutigen Algorithmen. Heutige Mitarbeitende in der IT verfügen in der Regel nicht über die hierfür notwendigen Skills. Es ist zu definieren, wann welche Skills für Quantencomputer in der eigenen IT-Abteilung benötigt werden. Auch Make-or-Buy-Entscheidungen hinsichtlich Hard- und Software müssen zukünftig ggf. anders getroffen werden. Hier steht der eigene IT-Bereich perspektivisch vor einem Transformationsprozess.

Neben diesen übergreifenden Querschnittsthemen können auch konkrete einzelne Handlungsfelder benannt werden. Diese sind in Abbildung 4 als Säulen dargestellt und werden im Folgenden näher erläutert.

1. Mit erster Priorität müssen Post-Quantum-Kryptographieverfahren eingeführt werden. Gemäß aktueller Experteneinschätzungen der Bafin ist davon auszugehen, dass alltagstaugliche Quantencomputer ab 2029 bzw. 2030 bereitstehen. Damit sind ab diesem Zeitpunkt herkömmliche Verschlüsselungsverfahren nicht mehr sicher. Da heute bereits Daten abgezogen und später entschlüsselt werden können (‚harvest now - decrypt later'), empfiehlt die Bafin, zeitnah PQC-Verfahren einzuführen. Es ist davon auszugehen, dass auch Prüfer in Kürze entsprechende Anforderungen, beispielsweise aus dem Digital Operational Resilience Act (DORA), so auslegen, dass die Verschlüsselungsverfahren auf PQC-Verfahren umgestellt werden müssen.

Aufgrund der sich schnell entwickelnden Technologie ist damit zu rechnen, dass laufend Anpassungen an den Schutzverfahren erforderlich sind. Deshalb ist gleichzeitig auch Quanten-Krypto-Agilität herzustellen, so dass der Austausch von Verschlüsselungsverfahren ohne grundlegende Anpassungen in der IT-Landschaft zukünftig möglich sein wird.

2. Im Gegensatz zur Post-Quantum-Kryptographie besteht noch keine Notwendigkeit, in der Breite auf Quanten-Kryptographieverfahren (QKD) umzustellen. Allerdings ist mittel- bis langfristig zu erwarten, dass insbesondere Zentralbanken, Clearingstellen und Börsen ausgewählte Datenübertragungen auf QKD-Verfahren umstellen werden. Deshalb ist es wichtig zu beobachten, welche Umstellungen geplant sind und dies beispielsweise frühzeitig im Zielbild der IT-Architektur zu berücksichtigen.
3. Ebenfalls ist zu prüfen, welche weiteren Use-Cases auf Quantencomputer bzw. Quantensoftware umzustellen sind. Bestimmte Use Cases (z.B. Monte-Carlo-Simulationen) eignen sich besonders für eine Umstellung auf Quantencomputer. Aktuell gibt es allerdings noch keine anwendungsreife Standardsoftware, es sind aber eine Vielzahl an Aktivitäten zur Entwicklung von überlegenen Quantenalgorithmen zu beobachten. Experten gehen davon aus, dass ab dem Jahr 2028 erste Use Cases auf Quantencomputern zu beobachten sein werden, die deutliche Wettbewerbsvorteile gegenüber Use Cases auf klassischen Rechnern liefern. Deshalb ist es zum einen wichtig, eine spezifische Perspektive zu entwickeln, welche für Quantencomputer geeignete Anwendungsfälle von besonderer geschäftspolitischer Bedeutung für das jeweilige Haus sind und gleichzeitig eine Markt- und Wettbewerberbeobachtung aufzusetzen, um Entwicklungen rechtzeitig zu erkennen.
4. Ergänzend kann geprüft werden, ob bis dahin hybride Algorithmen praktische Vorteile bieten. Hybride Algorithmen laufen auf herkömmlichen Rechnern, wenden aber Prinzipien von Quantensoftware an. Gegebenenfalls können hybride Algorithmen ein sinnvoller, mehrwertstiftender Zwischenschritt auf dem Weg zu echten Quantenalgorithmen sein.

Fazit: Kurzfristiger Handlungsbedarf

Die wichtigsten, kurzfristigen Handlungsbedarfe sind in Abbildung 5 zusammengefasst. Es wird empfohlen, mit erster Priorität bereits 2026 mit der Einführung von Post-Quantum-Kryptographieverfahren zu beginnen und die notwendige Quanten-Krypto-Agilität herzustellen, um die Kryptographieverfahren bei weiterem technischem Fortschritt mit möglichst geringem Aufwand anpassen zu können.

Hier ist es wichtig, zunächst eine Risikobewertung vorzunehmen und die Sachverhalte zu identifizieren, die als erstes geschützt werden müssen. Dann müssen die heutigen Kryptographieverfahren aufgenommen werden. Mit Hilfe einer Matrix kann eine Einordnung nach Schutzbedarf und aktuellem Schutzniveau erfolgen. Auf dieser Basis wird dann eine Bewertung vorgenommen und festgelegt, welche Übertragungswege in welcher Reihenfolge quantensicher zu schützen sind. Insgesamt ist zu beachten, dass die Umstellung auf Post-Quantum-Kryptographieverfahren deutlich komplexer ist als ein ‚Update' eines bisherigen Verschlüsselungsverfahrens.

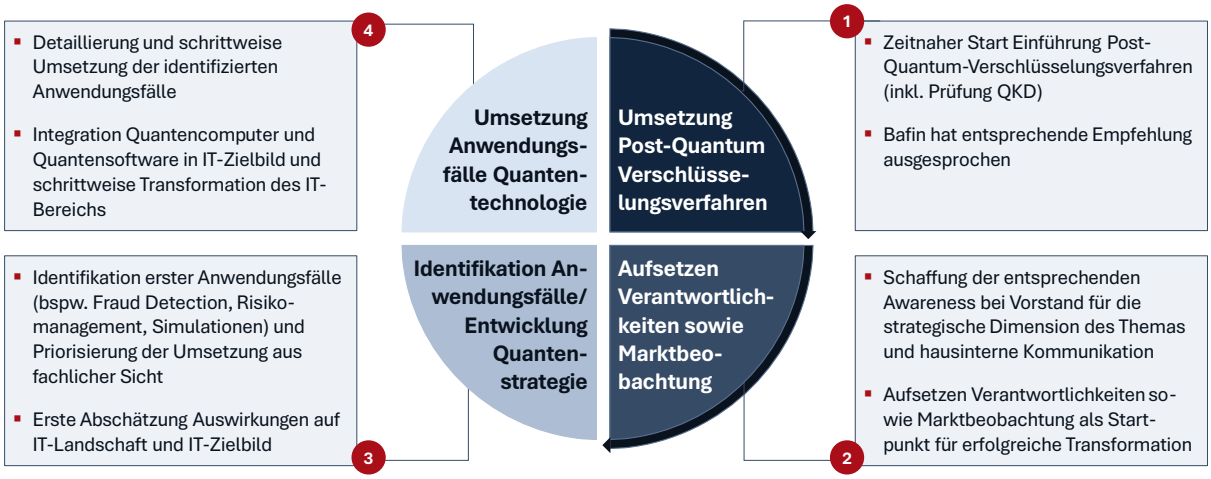


Abbildung 5 – Kurzfristiger Handlungsbedarf für Finanzdienstleister

Ebenso ist die Transformation hin zu Quantencomputern als strategisches Thema auf Vorstandsebene zu verankern, die Gesamtverantwortung inklusive der Verantwortlichkeit für Technologie-, Markt- und Wettbewerberbeobachtung unterhalb der Vorstandsebene zu definieren und schrittweise eine Gesamtstrategie zu entwickeln. Einzelne, gegebenenfalls bereits laufende Initiativen sind in diese Strategie zu integrieren. Aufgrund des technologisch und regulatorisch sich schnell ändernden Umfelds kann keine mehrjährige, starre Strategie entwickelt werden, sondern es muss eine laufend fortschreibbare Strategie definiert werden, die eng durch den Vorstand begleitet und laufend an neue technische Erkenntnisse angepasst werden kann.

Carsten Striebich ist Senior Manager bei EGC mit über 20 Jahren Erfahrung in der Beratung von Banken, Sparkassen, Versicherungen, Leasinggesellschaften und Asset-Managern. Sein Schwerpunkt liegt auf der Entwicklung von Geschäftsstrategien sowie großen Transformations- und Digitalisierungsprojekten. Bei EGC beobachtet er Entwicklung und Anwendung von Quantencomputern, Quantensoftware und Quantenverschlüsselungen und leitet den strategischen Handlungsbedarf für Finanzdienstleister ab.

Bisher erschienen:

#1 Dr. Marco Weiß – *Welt und Wesen des Datenmanagements*; September 2020

#2 Mario Kubik – *„DLT" – Potenzial zur Zukunftstechnologie?*; November 2020

#3 Jonathan Misler – *Verwendung von Daten und Modellen in datengetriebenen Geschäftsmodellen*; Januar 2021

#4 Johannes Bänsch – *Data Analytics und die Cloud*; März 2021

#5 Kurt Tanneberger – *Ja, wo sind sie denn? – Daten im IT-Betrieb*; Mai 2021

#6 Thomas Tiebor – *Data Governance als Fundament guten Datenmanagements;* Juli 2021

#7 Dr. Marco Weiß – *Artificial Intelligence – Nature or Nurture?*; September 2021

#8 Binjamin Sancar, Hermann Sgardelli – *Vertriebschancen in einer Bank durch Nutzung ihrer Daten und ihres Ökosystems;* November 2021

#9 Abdalla El Kadi – *Datenvisualisierung – eine Geschichte in Bildern;* Januar 2022

#10 Carsten Kuhlmann – *Kundenfokussierung: Daten und Technik*; März 2022

#11 Luca Winters – *CIEM – Cloud Infrastructure Entitlements Management*; Mai 2022

#12 Kristian Buric – *Der Informationsverbund - Daten (nur) für die Aufsicht?*; Juli 2022

#13 Stefan Bauer – *Aufbau eines SOC (Security Operations Center) als Kommandozentrale zur Cyberabwehr*; September 2022

#14 Thomas Tiebor – *Der Charme von IT-Datenarchitekturmustern;* November 2022

#15 Dr. Marco Weiß – *Citius, Altius, Fortius – Daten im Sport*; Januar 2023

#16 Simon Wilmerding – *Daten statt (nur) Bauchgefühl – Mit Datenanalysen den War for Talent gewinnen*; März 2023

#17 Kay Helbig – *ESG-Berichterstattung bei Versicherungen*; Mai 2023

#18 Dr. Marco Weiß – *Daten und Modelle in der 7. MaRisk-Novelle*; Juli 2023

#19 Fabio Giacomo Müller – *Softwareeinführungsprojekte im internationalen Kontext*; September 2023

#20 Stefan Bauer – *Digital Operational Resilience Act (DORA): Wie hoch wird die nächste Welle der Regulierung?*; November 2023

#21 Prof. Dr. Hans-Gert Penzel – *Tokenisierung von Vermögenswerten: Wie die Zukunft des Eigentums aussehen wird*; Januar 2024

#22 Andreas Sperlich – *Ehrlich bleiben bei der Kundenzufriedenheitsmessung: Die Schlüsselrolle von Integrität und Authentizität;* März 2024

#23 Tomislav Bisic, Simon Wilmerding – *Keine KI ist auch keine Lösung – in der ESG-Berichterstattung*; Mai 2024

#24 Stefan Schnitzler – *Die Rolle der Daten im Retail Payment*; Juli 2024

#25 Sören Bey, Simon Wilmerding – *Robuste Datenarchitektur: Das Fundament für effektiven KI-Einsatz*; September 2024

#26 Mark Wieczorrek – *Effektive Kundendaten-Governance: Der Schlüssel zu nachhaltigem Geschäftserfolg*; November 2024

#27 Sören Bey, Simon Wilmerding – *Skalierung von KI-Lösungen bei Finanzdienstleistern*; Januar 2025

#28 Dr. Marco Weiß – *Business Intelligence-Strategie – Wertschöpfung aus Daten*; März 2025

#29 Stefan Schnitzler, Dr. Rainer Schamberger – *Vom Datensilo zum Daten-Ökosystem: Warum FiDA eine große Chance ist, den Kunden in den Mittelpunkt zu rücken*; Mai 2025

#30 Kay Helbig, Jörg Dreinhöfer – *Rückgrat der modernen IT – Mainframe?*; Juli 2025

#31 Hauke Hinderlich – *Daten in Finanzen und Radsport: Auf dem Weg zu besserer Performance*; September 2025

#32 Carsten Striebich – *Quantencomputer – Überblick über Status und Handlungsbedarf*; November 2025

Über den DataNavigator

Unterschiedliche Autoren beleuchten in der Reihe DataNavigator die vielfältigen Facetten des Datenmanagements und zeigen Ihnen interessante Aspekte auf.

Der DataNavigator wird von Eurogroup Consulting regelmäßig zweimonatlich herausgegeben und möchte Ihnen interessante Denkanstöße liefern. Wir freuen uns, Ihnen mit dem DataNavigator unsere Erfahrungen weiterzugeben und stehen Ihnen für die Diskussion gerne zur Verfügung!

Sie erreichen Autoren und Herausgeber bei Anregungen und Feedback unter der E-Mail-Adresse datanavigator@eurogroupconsulting.de.