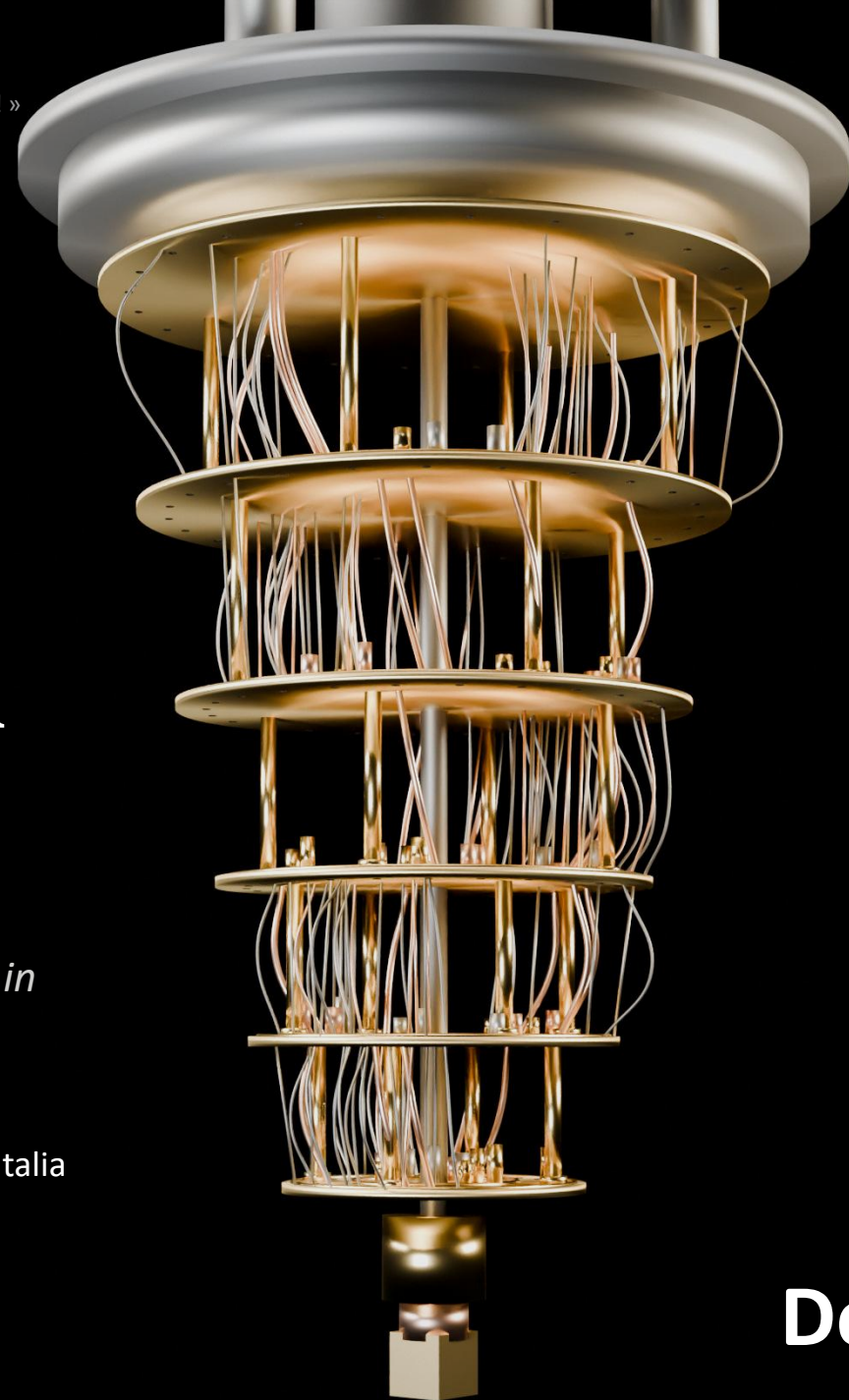


La transizione quantistica nei sistemi finanziari

Computer quantistici, comunicazione quantistica e crittografia post-quantum (PQC): la strategia di gruppo che le banche devono portare in Consiglio, tra protezione, valore, competenze e norme.

Tommaso Stranieri, Partner, Deloitte, Digital Regulation Leader e Quantum Leader Italia



Il percorso in cinque passaggi

Che cosa cambia per chi decide, che cosa chiedono le autorità, a che punto è la banca, quale strategia portare in Consiglio e con quali competenze, tecnologie, partner e investimenti.

01

Perché ora

Che cosa è cambiato in dodici mesi; valore e rischio per chi decide; vita utile dei dati; dati cifrati oggi, leggibili domani

02

Le attese

Richieste e scadenze di BCE, Banca d'Italia, ACN, Unione europea e G7

03

Maturità e competenze

A che punto è la banca sulle due famiglie di competenze; governance, profili, come dotarsene

04

La strategia

Sette linee d'azione; su quali tecnologie puntare e con quali partner

05

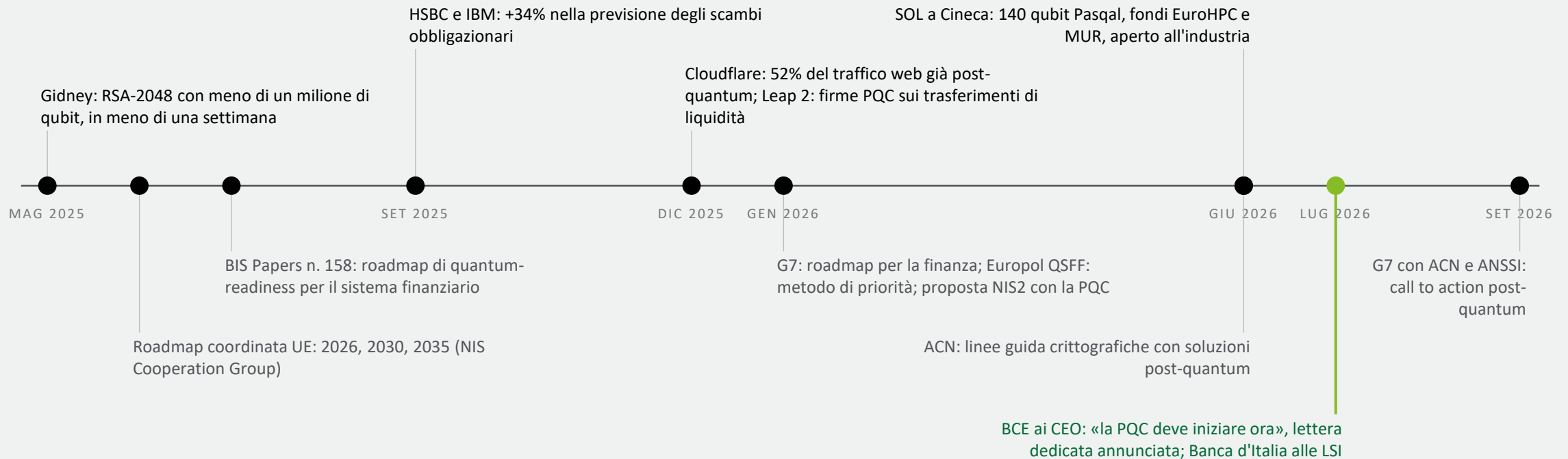
Le opzioni

Tre opzioni per il Consiglio: perimetro, tempi, investimenti, rischio residuo

Che cosa è cambiato negli ultimi dodici mesi

Tra maggio 2025 e settembre 2026 la stima dell'attacco si è ridotta, la migrazione dei canali è iniziata, le prime macchine sono arrivate in Italia e le autorità hanno sostituito le raccomandazioni con richieste e scadenze precise.

TECNOLOGIA E MINACCIA SOPRA L'ASSE, NORME E VIGILANZA SOTTO



Valore e rischio in banca: le otto dimensioni

Otto dimensioni, ciascuna con un responsabile. Per la crittografia c'è una scadenza, per le altre un costo o un'opportunità; dalle competenze dipende il governo delle altre sette. Il Consiglio le deve valutare insieme.

OTTO DIMENSIONI PER IL COMITATO ESECUTIVO E IL Consiglio		
DIMENSIONE E RESPONSABILE	● VALORE	● RISCHIO
Crittografia e dati CISO · CIO · CDO	PQC e QKD danno una protezione duratura a canali, firme e archivi.	Shor rompe la chiave pubblica; dati raccolti oggi e decifrati domani; firme passate falsificabili e contratti ripudiabili.
Cyber-resilienza CISO · CRO	Simulare propagazione e isolamento degli attacchi; AI difensiva generativa; stress test dell'architettura.	AI offensiva adattiva, attacchi di propagazione ottimizzati, ricerca automatica di vulnerabilità.
Business e mercati CEO · CFO · BUSINESS	Ottimizzazione di portafogli e liquidità, pricing di derivati, trading potenziato: HSBC e IBM, +34% (2025).	Chi arriva prima sui casi d'uso acquisisce un vantaggio informativo sui mercati a scapito degli altri.
Rischio, frodi, credito CRO · CCO	QML per antiriciclaggio e antifrode, credit scoring, scenari di stress sintetici per il VaR.	Modelli opachi e bias amplificati, in attrito con AI Act, GDPR e vigilanza sulle decisioni automatizzate.
Dati e modelli CDO · CRO	Classificare i dati per vita utile e prepararli al QML: qualità, tracciabilità, spiegabilità.	Archivi a vita lunga (KYC, sanitari, biometrici) esposti oggi; governance dei modelli non pronta.
Tecnologia, fornitori, costi CIO · PROCUREMENT · CFO	Accesso via cloud e HPC pubblico senza possedere macchine; agilità crittografica utile anche dopo la migrazione.	Migrazione multimilionaria dei sistemi legacy; dipendenza da pochi fornitori di cloud quantistico, HSM e PKI.
Norme, vigilanza, stabilità CCO · CRO · Consiglio	Conformità anticipata a DORA, NIS2 e attese BCE; efficienza energetica dei modelli (ESG).	Scadenze 2026, 2030 e 2035 con rilievi di vigilanza; oligopolio tecnologico e stabilità dei mercati.
Competenze e organizzazione CHRO · CIO · CISO	Due famiglie di competenze, casi d'uso e quantum-safe, da costruire adesso, mentre i profili sono ancora reperibili.	Profili scarsi, dipendenza da consulenti e fornitori, scelte tecnologiche senza chi le sappia valutare.

I dati della finanza: volumi e durata della riservatezza

I volumi crescono più in fretta di quanto si riesca a migrare, e molti archivi devono restare riservati oltre la finestra 2030-2035: per questi ultimi il rischio esiste già oggi.

I NUMERI DEL SISTEMA

150 mld

pagamenti non in contanti nell'area dell'euro nel 2024, per 230.000 miliardi di euro (BCE)

4 mld

operazioni non in contanti in Italia nel solo quarto trimestre 2025, +45% in tre anni (Banca d'Italia)

53 mln

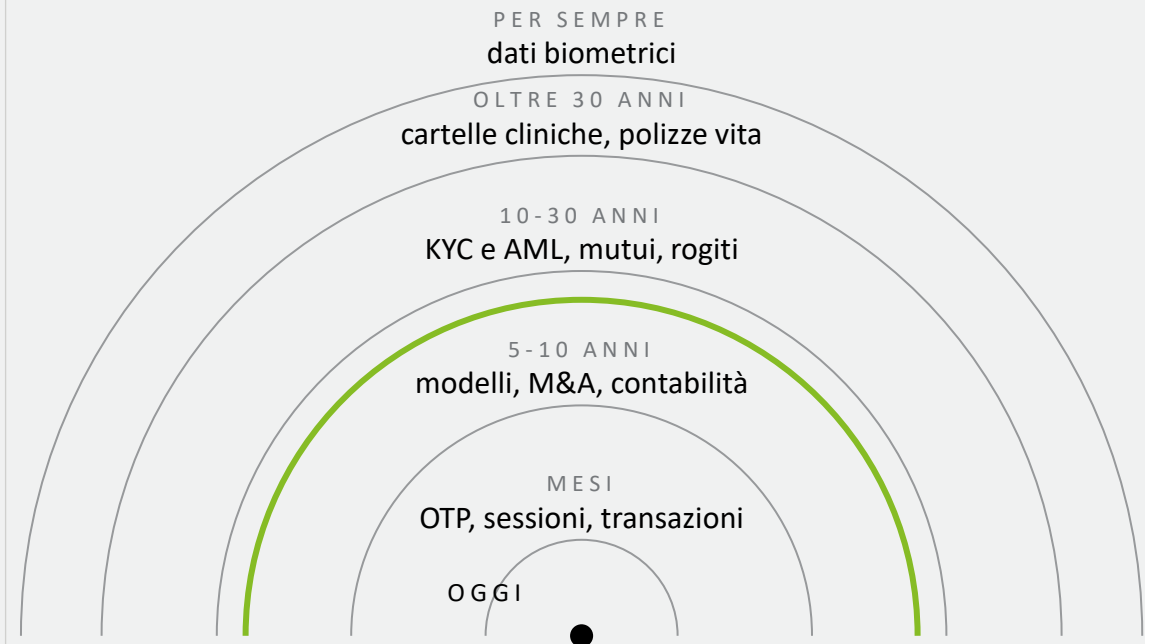
messaggi al giorno sulla rete Swift, tra 11.500 istituzioni

394 ZB

dati nel mondo nel 2028, da 149 nel 2024: il patrimonio da cifrare cresce più in fretta della migrazione (IDC)

PER QUANTO DEVONO RESTARE SEGRETI: ORBITE DI VITA UTILE

Anello verde: finestra di rischio 2030-2035. Oltre l'anello, i dati copiati oggi sono già esposti.



Dati cifrati oggi e leggibili domani

In transito quasi tutto è cifrato, e per questo viene raccolto; a riposo metà dei dati sensibili non lo è. Le priorità di migrazione vanno fissate insieme al business.

QUANTO È CIFRATO, QUANTO È PRONTO

traffico web già post-quantum, dicembre 2025



dati sensibili in cloud cifrati



sanno dove risiedono tutti i propri dati



temono la decifratura futura dei dati



sperimentano già gli algoritmi post-quantum



In verde: traffico web umano già protetto da scambio di chiavi post-quantum.



Critica, entro 12 mesi

Identità e KYC, dati sanitari e polizze vita, custodia di digital asset.



Alta, entro 2 anni

Pagamenti e messaggistica interbancaria, home banking, modelli proprietari.



Media, entro 3 anni

Firmware di ATM e POS, mutui e rogiti, archivi immobiliari.

Richieste delle autorità e scadenze

Le norme non prescrivono un algoritmo. Richiedono però che la banca sappia dove usa la crittografia, chi ne risponde e quando intende sostituirla.

NORMA	CHE COSA CHIEDE	DATA
DORA e RTS (UE) 2024/1774	Politica di cifratura e gestione delle chiavi; aggiornamento secondo la crittanalisi; registro dei certificati per le funzioni critiche	17 gennaio 2025
NIS2 e d.lgs. 138/2024	Crittografia tra le misure minime; responsabilità degli organi di amministrazione; proposta COM(2026) 13: politiche nazionali di transizione	16 ottobre 2024
Roadmap europea PQC	Avvio e primi passi; casi d'uso ad alto rischio migrati; il maggior numero possibile di sistemi	2026, 2030, 2035
G7 Cyber Expert Group	Roadmap per il settore finanziario: prima i sistemi critici, poi il resto; call to action di settembre 2026	2030-2032, 2035
ACN, Linee guida crittografiche	Firme digitali, cifrari a flusso e linea guida TLS versione 2.0 con soluzioni post-quantum; inventario e schemi ibridi	15 giugno 2026
BCE, lettera del 7 luglio 2026	Piani d'azione AI e cyber con responsabili, risorse e tempi; «la PQC deve iniziare ora»; lettera dedicata al quantum annunciata	31 ottobre 2026

La maturità della banca su due famiglie di competenze

La maturità si misura su due assi: saper trovare i casi d'uso e saper rendere sicura la crittografia. Il primo passo dipende dal quadrante, più che dall'ambizione.

QUATTRO PROFILI E IL PRIMO PASSO PER CIASCUNO

COMPETENZE DI BUSINESS: CASI D'USO



Esploratore

Laboratorio attivo sui casi d'uso; crittografia non inventariata.

Primo passo: CBOM, QRA, migrazione ibrida dei canali.



Pioniere

Le due famiglie integrate in una strategia di gruppo con riporto al Consiglio.

Primo passo: portafoglio di partner, prodotti quantum-safe.



Osservatore

Nessun presidio; la PQC vissuta come conformità futura.

Primo passo: un responsabile, l'inventario, formazione di base.



Difensore

Cyber presidiata: inventario e QRA avviati; nessun caso d'uso.

Primo passo: laboratorio via cloud, primo caso d'uso di business.

BASSE

COMPETENZE QUANTUM-SAFE: CRITTOGRAFIA E CYBER

ALTE

CINQUE DOMANDE PER COLLOCARSI

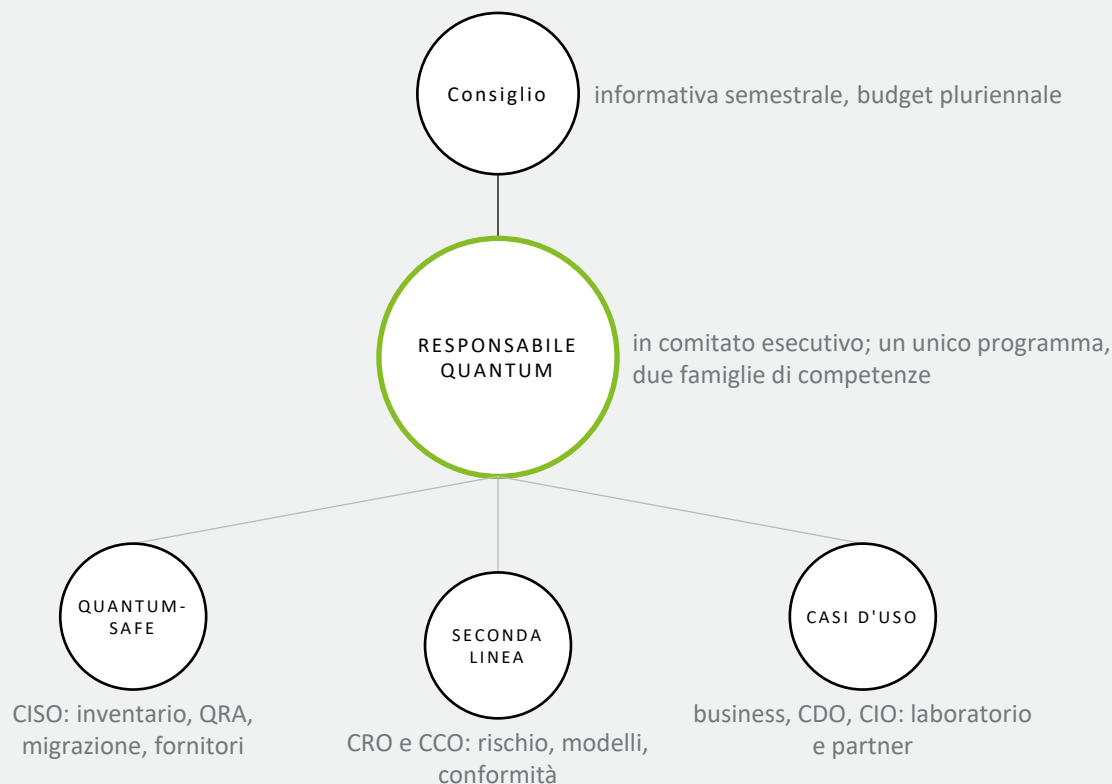
- 1 C'è un responsabile del rischio quantistico in comitato esecutivo?
- 2 Esiste un inventario crittografico leggibile dalle macchine (CBOM)?
- 3 Quanti casi d'uso di calcolo quantistico sono stati provati in dodici mesi?
- 4 Quante persone hanno competenze quantistiche o quantum-safe, e dove riportano?
- 5 Il Consiglio ha ricevuto un'informativa sul quantum negli ultimi dodici mesi?

Nel nostro osservatorio la maggior parte degli intermediari italiani sta tra Osservatore e Difensore; poche grandi banche sono Pionieri.

Governance e competenze: ruoli, profili e come dotarsene

Un responsabile in comitato esecutivo che riferisce ogni sei mesi al Consiglio, un unico programma per le due famiglie di competenze e un modo realistico per dotarsene: formazione interna, poche assunzioni senior, alleanze.

MODELLO ORGANIZZATIVO E PROFILI



PROFILI DA COSTRUIRE

Architetto quantum-safe

inventario, HSM e PKI, agilità crittografica, migrazione ibrida

Analista del rischio quantistico

QRA per caso d'uso, terze parti, riporto alla seconda linea

Specialista di casi d'uso

ottimizzazione, QML, pricing; lavora con il business

Gestore di partner e fornitori

cloud e HPC, università, clausole post-quantum

COME DOTARSENE

Formazione interna di cyber e data science (le basi in sei mesi); poche assunzioni senior; alleanze con università e PNRR (ICSC Spoke 10, SERICS) e con i programmi dei fornitori; consulenza solo per la diagnosi. Da 2-3 persone per un Osservatore a 8-10 per un Pioniere.

Sette linee d'azione per la strategia quantistica di gruppo

La protezione post-quantum è la sola linea con una scadenza; dalle altre sei dipende se la banca subirà il cambiamento o ne trarrà vantaggio. Un responsabile, due famiglie di competenze e un riporto periodico al Consiglio.

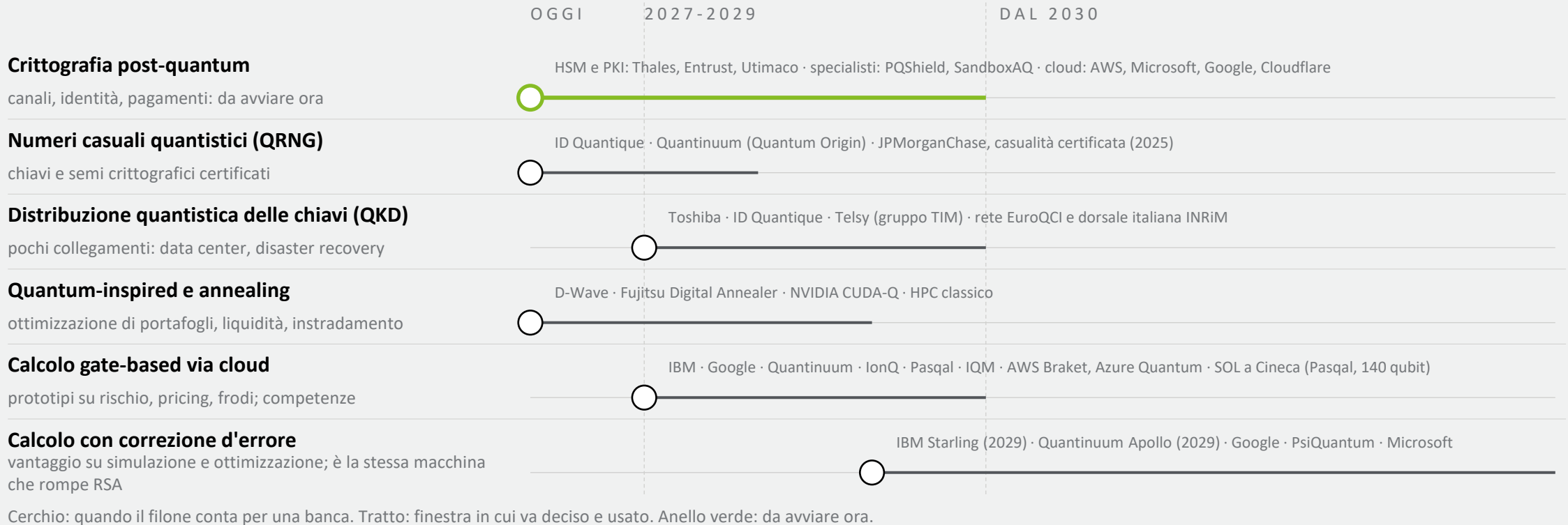
SOPRA LA LINEA CHE COSA FARE, SOTTO CON QUALI MEZZI



Tecnologie e alleanze: sei filoni e i relativi fornitori

Un portafoglio di tecnologie anziché una sola scommessa: software post-quantum e numeri casuali subito; calcolo via cloud e HPC pubblico per costruire competenze; correzione d'errore dopo il 2029. I nomi indicati sono soltanto esemplificativi

SEI FILONI: QUANDO CONTANO PER UNA BANCA, CON QUALI FORNITORI



Tre opzioni per il Consiglio: perimetro, tempi, investimenti

Ordini di grandezza stimati dello spending per un intermediario di media dimensione in quattro anni, da calibrare con l'inventario; per un gruppo significativo, tre-cinque volte tanto.

TRE OPZIONI, STESSO RESPONSABILE E STESSO RIPORTO SEMESTRALE

A Conformità

2-5 M€

IN QUATTRO ANNI, ORDINE DI GRANDEZZA
PERIMETRO

Solo protezione: inventario, QRA, migrazione ibrida ad alto rischio, clausole; 2-3 profili quantum-safe.

TEMPI

Piano nel 2026; alto rischio entro il 2030; il resto entro il 2035.

CHE COSA OTTIENE

Conformità a DORA, NIS2 e attese BCE; rischio HNDL ridotto sui dati a vita lunga.

RISCHIO RESIDUO

Nessuna capacità sul valore; dipendenza dai fornitori; competenze da comprare dopo.

B Equilibrata

5-10 M€

IN QUATTRO ANNI, ORDINE DI GRANDEZZA
PERIMETRO

Protezione completa più un laboratorio di 3-5 persone: cloud e HPC, 2-3 casi d'uso l'anno, pilota QKD.

TEMPI

Come A; primo caso d'uso nel 2027, pilota QKD nel 2028, decisione sulla correzione d'errore nel 2030.

CHE COSA OTTIENE

Conformità, competenze interne, opzioni reali sul valore, credibilità con vigilanza e fornitori.

RISCHIO RESIDUO

Laboratorio ricorrente, 1-1,5 M€ l'anno; risultati di business non garantiti prima del 2030.

C Leadership

10-20 M€

IN QUATTRO ANNI, ORDINE DI GRANDEZZA
PERIMETRO

Come B, più un team di 8-10 persone, HPC e on-premise, QKD sui collegamenti critici, prodotti quantum-safe.

TEMPI

Team e HPC nel 2027; prodotti quantum-safe nel 2028; macchine con correzione d'errore dal 2029-2030.

CHE COSA OTTIENE

Vantaggio competitivo e reputazionale; ruolo attivo nell'ecosistema europeo; anticipo sul mercato.

RISCHIO RESIDUO

Investimento e incertezza tecnologica; rischio di puntare sulla modalità sbagliata senza portafoglio.

Tre decisioni per il Consiglio

Approvare la strategia e nominare il responsabile entro il 2026; proteggere i dati a vita lunga entro il 2030; costruire da subito competenze, tecnologie e alleanze.

● Entro il 2026: approvare la strategia e nominare

Strategia quantistica di gruppo, responsabile in comitato esecutivo e budget pluriennale; nel piano d'azione del 31 ottobre, evidenza della PQC in corso.

○ Entro il 2030: dati a vita lunga protetti

Inventario e QRA subito; canali, identità, pagamenti e archivi a vita lunga migrati in modalità ibrida; agilità crittografica richiesta ai fornitori.

○ Da oggi: competenze, tecnologie e partner

Due famiglie di competenze da costruire, un portafoglio di sperimentazioni via cloud e HPC pubblico, alleanze con fornitori e università.

Il tempo è una variabile crittografica. Chi lo misura oggi decide; chi lo ignora lo subisce.