# QUANTUM READINESS: DA DOVE INIZIARE?

## DALLA CONSAPEVOLEZZA ALLA STRATEGIA: PREPARARE OGGI LA SICUREZZA DI DOMANI

WHITE PAPER DI ANTEPRIMA AL WEBINAR AUSED IN COLLABORAZIONE CON ITALTEL
16 SETTEMBRE 2026 | TLP: CLEAR

**Executive view**

L'evoluzione del Quantum Computing sta suscitando un sempre maggiore interesse nelle agende del top management delle aziende. L'avvento del quantum computer, infatti, metterà a disposizione una potenza di calcolo tale da invalidare anche le più solide difese informatiche.

Ad oggi la disponibilità di un computer quantistico crittograficamente rilevante resta incerta nei tempi, ma i risultati sperimentali mostrano una continua accelerazione delle roadmap. I tempi necessari per adeguare infrastrutture, applicazioni, certificati, identità digitali, VPN, sistemi legacy, ambienti cloud e processi di governance, sono invece una variabile misurabile e strategica e richiedono tempestività nell'azione.

**In questo scenario potenzialmente disruptive è fondamentale porsi la domanda: "Se domani fosse necessario sostituire o affiancare RSA ed ECC nei sistemi critici, quanto tempo servirebbe alla nostra organizzazione per farlo mantenendo la continuità dei servizi?"**

CIO e CISO sono in prima linea come responsabili della gestione del rischio, dell'implementazione della sicurezza digitale e della governance crittografica e, anche in questa fase di forte discontinuità tecnologica, devono operare per garantire alle loro organizzazioni continuità operativa, compliance, protezione degli investimenti, resilienza delle infrastrutture digitali e capacità di adattamento a standard e minacce in continua evoluzione.

Per raggiungere questi obiettivi, le organizzazioni dovranno trasformare una potenziale discontinuità tecnologica in un percorso governato, progressivo e coerente con il loro profilo di rischio mantenendosi aperte alle evoluzioni future di minacce, standard e tecnologie (Crypto-Agility). Chiameremo questo stato di prontezza: "**Quantum Readiness".**

Da qui parte il percorso: assesment, prioritizzazione, roadmap e adozione progressiva di architetture quantum-safe e crypto-agile.

## 1. Perché iniziare oggi?

La crittografia protegge comunicazioni, dati, identità, certificati, applicazioni e transazioni. L'evoluzione del quantum computing rende necessario preparare per tempo l'adeguamento degli algoritmi oggi più diffusi, in particolare RSA ed ECC.

Per CIO e CISO, un punto centrale è stimare il tempo richiesto all'organizzazione per conoscere, modificare e governare la propria infrastruttura crittografica in vista del cosiddetto Q-Day.

Tra gli scenari da considerare rientra anche il rischio **Harvest Now, Decrypt Later**: dati cifrati oggi potrebbero essere conservati e decifrati in futuro. Il tema si inserisce nella valutazione di durata della riservatezza, criticità dei servizi e tempi di migrazione.

Il paradigma evolve: dalla sicurezza basata sulla robustezza statica degli algoritmi si passa a una sicurezza progettata per cambiare nel tempo, capace di adattarsi a nuove minacce, standard e tecnologie.

Per CIO e CISO, la Quantum Readiness diventa la capacità di governare il cambiamento, rendendo sicurezza e infrastrutture adattabili nel tempo.

La Quantum Readiness sposta l'attenzione dalla previsione alla preparazione. Il rischio dipende dalla maturità del quantum computing e dal tempo richiesto dall'organizzazione per modificare sistemi, applicazioni, protocolli, certificati e processi di sicurezza.

La decisione da prendere oggi riguarda le capacità da costruire per evolvere in modo controllato e adattivo: governance, inventario, prioritizzazione, roadmap.

## 2. Dove siamo oggi: maturità tecnologica e Readiness organizzativa

L'evoluzione del quantum computing procede lungo diverse fasi di maturità. Oggi sono disponibili processori quantistici e sistemi NISQ – Noisy Intermediate-Scale Quantum – caratterizzati da qubit fisici ancora soggetti a rumore ed errori. La transizione verso sistemi fault-tolerant richiede lo sviluppo di qubit logici affidabili, ottenuti attraverso tecniche di correzione degli errori.

Il passaggio successivo è rappresentato da sistemi fault-tolerant scalabili, in grado di operare con un numero sufficiente di qubit logici stabili. Questa è una milestone fondamentale per realizzare il primo CRQC – Cryptographically Relevant Quantum Computer – cioè un computer quantistico con capacità tali da compromettere algoritmi di crittografia asimmetrica oggi ampiamente utilizzati.

Per le organizzazioni, il tema si declina in 2 fronti:

- Esterno: la continua evoluzione fino alla maturità della tecnologia quantistica, hardware, qubit, correzione degli errori, scalabilità e mercato.
- Interno: la Readiness dell'organizzazione intesa come governance, inventario crittografico, dipendenze, competenze, roadmap, fornitori e capacità di cambiamento.

Dei due fronti, già il solo progresso sempre più veloce della tecnologia fa nascere l'esigenza di agire da subito: quando la migrazione richiede anni, la pianificazione deve iniziare prima che la pressione diventi emergenziale.

## 3. Il fattore tempo: dalla previsione alla preparazione

Se il Q-Day rimane una data sconosciuta, per le organizzazioni esistono alcune variabili già note/governabili che consentono di iniziare il processo di analisi:

1. **la durata della riservatezza dei dati**
2. **la capacità decisionale dell'organizzazione**
3. **"crypto-rigidity": sistemi legacy, dipendenze tecnologiche, componenti proprietari e filiere complesse che influenzano il tempo di migrazione**

La Quantum Readiness nasce dall'intersezione di queste dimensioni. Quando un'informazione deve rimanere riservata per molti anni e l'organizzazione richiede anni per adeguare sistemi e applicazioni, la finestra di preparazione può essere più breve di quanto sembri.

**Il rischio più concreto è scoprire troppo tardi che l'infrastruttura crittografica richiede anni per essere modificata.**

La combinazione di questi criteri consente al management di formulare una prima mappa delle priorità di intervento e supportare la costruzione di una roadmap di migrazione.

## 4. Il percorso di execution verso la Quantum Readiness

La roadmap traduce i risultati dell'assesment in priorità, sequenza degli interventi, dipendenze, responsabilità, tecnologie da valutare, milestone e criteri di verifica. Integrata nei cicli di rinnovo tecnologico, nei programmi di modernizzazione applicativa e nei progetti infrastrutturali, permette di distribuire nel tempo attività e investimenti mantenendo il controllo sul rischio.

Il perimetro della migrazione comprende applicazioni, server, VPN, certificati, PKI, dispositivi, sistemi legacy, cloud, infrastrutture di rete e fornitori.

Per CIO e CISO, il risultato atteso è una capacità permanente di governo: riduzione del rischio, protezione degli investimenti, maggiore resilienza e capacità di adattarsi nel tempo all'evoluzione di standard, minacce e tecnologie.

La composizione della roadmap richiede di prendere decisioni su tre piani:

- **architetture crypto-agile** progettate per rendere la crittografia modulare ed evolvibile;
- **governance centralizzata** di chiavi, certificati, responsabilità, budget e metriche;
- **coinvolgimento strutturato di fornitori**, cloud provider, partner tecnologici e supply chain.

Nello specifico la "crypto-agility" rappresenta un elemento trasversale al percorso: architetture modulari, policy, versioning, gestione delle dipendenze, automazione del ciclo di vita, test e strategie di migrazione consentono di incorporare nuovi meccanismi di sicurezza con impatto controllato su applicazioni e servizi.

L'esecuzione strutturata di questo processo è fondamentale per portare l'azienda verso la Quantum Readiness.

## 5. Le tecnologie per la quantum-safe security

| Tecnologia | Ruolo nel percorso | Priorità di valutazione |
|---|---|---|
| PQC | Baseline crittografica della transizione quantum-safe. | Allineamento con roadmap applicative, piani di aggiornamento e profilo di rischio. |
| QKD | Opzione infrastrutturale per collegamenti ad alta criticità. | Coerenza con criticità dei collegamenti, vincoli infrastrutturali e sostenibilità del modello operativo. |
| SKE / DSKE | Approccio complementare per rafforzare la distribuzione sicura delle chiavi. | Rilevanza per governance delle chiavi, scalabilità e architetture ibride. |

La tabella offre una lettura orientata alle scelte, lasciando al webinar l'approfondimento tecnico su principi di funzionamento, vantaggi, vincoli e scenari di adozione.

## 6. Standard e compliance

La transizione quantum-safe si sviluppa in parallelo all'evoluzione degli standard internazionali.

Per il management, i riferimenti da monitorare riguardano standard tecnologici, linee guida operative, compliance, regolazione e modelli di maturità.

In un contesto dinamico, la standardizzazione richiede la capacità di monitorare gli aggiornamenti, recepire nuovi profili tecnici e valutarne l'impatto sulle architetture esistenti.

La Quantum Readiness deve quindi includere un presidio continuo sull'evoluzione regolatoria, tecnica e di compliance.

NIST, ETSI, IETF, BSI, ENISA, GSMA, NIS2 e DORA rappresentano i principali riferimenti che contribuiscono a definire il quadro di standardizzazione, best practice e compliance.

Standard e compliance diventano parte della governance: influenzano architetture, procurement, requisiti verso i fornitori, programmi di modernizzazione, gestione del rischio e piani di continuità.

## 7. Strategie diverse per una sfida globale

La transizione quantum-safe è entrata nelle agende strategiche internazionali, con approcci che riflettono priorità diverse: standardizzazione software, gestione del rischio, coordinamento istituzionale, investimenti infrastrutturali e controllo della supply chain.

Per CIO e CISO, le roadmap nazionali offrono una lettura operativa convergente sull'esigenza di avviare assesment, prioritizzazione e pianificazione della migrazione crittografica.

| Area | Orientamento prevalente | Rilevanza strategica |
|---|---|---|
| USA | Software-first e standardizzazione PQC. | Priorità a inventario crittografico, impatto applicativo e capacità di aggiornamento. |
| Canada | Transizione guidata da rischio e criticità dei sistemi. | Allineamento tra rischio, priorità di business e roadmap di migrazione. |
| Unione Europea | Coordinamento istituzionale e approccio ibrido. | Integrazione tra standard, compliance, resilienza e trasformazione digitale. |
| Regno Unito | Governance centralizzata e priorità agli asset critici. | Presidio centralizzato di responsabilità, milestone e avanzamento. |
| Asia | Investimenti infrastrutturali e sviluppo di capacità nazionali. | Rilevanza per infrastrutture critiche, connettività, cloud distribuito ed ecosistemi nazionali. |
| Australia | Approccio basato su rischio e supply chain. | Centralità di fornitori, dipendenze digitali, supply chain e continuità operativa. |

**Messaggio chiave -** Le diverse strategie internazionali indicano una stessa direzione manageriale: la transizione quantum-safe richiede visibilità sugli asset, capacità di pianificazione, gestione della supply-chain e integrazione nelle strategie di resilienza.

## 8. L'esperienza Italtel

Il percorso di Italtel nella quantum security integra ricerca, sperimentazione e system-integration. L'esperienza maturata negli ultimi anni include attività su QKD, reti SDN, reti ottiche metropolitane, protezione di dati sanitari, Post-Quantum Cryptography su reti B5G (Beyond 5G), architetture ibride, crypto-agility, laboratori dedicati e PoC.

Nel 2026 il percorso comprende attività di validazione quantum-safe su reti e infrastrutture critiche attraverso progetti commerciali nell'ambito bancario e telco e in progetti di ricerca, nell'ambito delle reti mission critical delle utilities (progetto **IT GEMINI)** e in ambito telco e automotive per la validazione di soluzioni PQC (progetto **EU SMARTY)**.

L'approccio Italtel è orientato all'integrazione progressiva di tecnologie quantum-safe nelle infrastrutture esistenti. L'obiettivo è introdurre nuove capacità di protezione preservando continuità operativa, interoperabilità, scalabilità e protezione degli investimenti.

Le competenze si traducono in soluzioni orientate all'integrazione: piattaforme *crypto-agile* per combinare PQC, DSKE e QKD con apparati e infrastrutture esistenti, supportando collegamenti protetti, security hub, reti multi-cloud e servizi quantum-safe.

La prospettiva evolutiva si estende oltre la migrazione iniziale: “quantum-safe everywhere”, architetture ibride e *crypto-agile*, security as-a-service e sicurezza supportata dall’AI indicano una traiettoria in cui la resilienza dipende dalla capacità continua di evolvere.

## 10. Tre domande da portare al webinar

In vista del webinar può essere utile cominciare a porsi le seguenti domande:

**1. Quanto tempo servirebbe alla nostra organizzazione per sostituire o affiancare RSA ed ECC nei sistemi critici mantenendo la continuità dei servizi?**

**2. Conosciamo realmente il nostro patrimonio crittografico, incluse dipendenze applicative, certificati, chiavi, PKI, fornitori e sistemi legacy?**

**3. Quali dati, comunicazioni e identità digitali devono rimanere protetti per un orizzonte temporale superiore a quello in cui potrebbe emergere un primo CRQC (Cryptographic Relevant Quantum Computer)?**

Queste domande aiutano a condurre il tema dal piano tecnologico a quello decisionale, concentrando l’attenzione sul livello di preparazione dell’organizzazione a cambiare quando sarà necessario.

## 11. Dal white paper al webinar: trasformare la consapevolezza in decisione

Questo white paper apre il confronto su una decisione che entrerà progressivamente nell’agenda di ogni organizzazione digitale: preparare oggi la resilienza crittografica necessaria per proteggere dati, identità, infrastrutture e servizi nel tempo.

Il webinar AUSED, in collaborazione con Italtel, porterà il tema sul piano delle scelte executive: comprendere il livello di esposizione, identificare le priorità, valutare le tecnologie quantum-safe e impostare una roadmap sostenibile, integrata con governance, compliance, procurement, architetture e continuità operativa.

**La domanda non è quando arriverà il cambiamento, ma quanto l’organizzazione sarà pronta a governarlo.**

## Appendice — vocabolario essenziale

**Qubit**
Unità fondamentale dell'informazione quantistica.

**Physical qubit**
Qubit realizzato fisicamente, soggetto a rumore ed errori.

**Logical qubit**
Qubit ottenuto combinando più qubit fisici attraverso tecniche di correzione degli errori, con l'obiettivo di aumentarne l'affidabilità.

**Fault-tolerant quantum computing**
Calcolo quantistico progettato per operare con livelli di errore sufficientemente bassi grazie alla correzione degli errori.

**CRQC - Cryptographically Relevant Quantum Computer**
Computer quantistico con capacità sufficienti a compromettere alcuni algoritmi crittografici oggi utilizzati.

**Q-Day**
Termine utilizzato per indicare il momento in cui tali capacità potrebbero diventare concretamente disponibili.

**Quantum Readiness**
Capacità strategica dell'organizzazione di preparare, governare e rendere sostenibile nel tempo l'adeguamento della propria crittografia all'evoluzione di minacce, standard e tecnologie.

**PQC - Post-Quantum Cryptography**
Algoritmi crittografici progettati per resistere anche ad attacchi condotti con computer quantistici.

**QKD - Quantum Key Distribution**
Tecnologia per la distribuzione delle chiavi crittografiche basata su proprietà della meccanica quantistica.

**Crypto-agility**
Capacità di aggiornare, sostituire o introdurre componenti crittografici con un impatto controllato su applicazioni e servizi.

**Quantum-safe security**
Insieme di tecnologie, architetture e pratiche che proteggono dati, comunicazioni e identità dalle minacce abilitate dal quantum computing, sostenendo continuità e resilienza.

**Harvest Now, Decrypt Later**
Scenario di rischio in cui dati cifrati vengono raccolti oggi per essere decifrati in futuro, quando saranno disponibili capacità di calcolo adeguate.

**Crypto-rigidity**
Difficoltà strutturale di modificare o sostituire componenti crittografici a causa di sistemi legacy, dipendenze tecnologiche, componenti proprietari o processi di aggiornamento complessi.