

Hybrid quantum infrastructure checklist

CATEGORY	CHECKLIST ITEM	NEXT STEPS
1. STRATEGIZE	Define phased quantum roadmap	• Set short-, medium- and long-term quantum objectives. • Identify required milestones (C-suite support, funding, infrastructure upgrades). • Assign owners for each milestone and establish KPIs.
	Secure executive and enterprise buy-in	• Prepare briefing materials outlining risks, benefits and ROI. • Align quantum strategy with existing digital transformation goals. • Present budget requirements and timelines.
	Plan infrastructure evolution	• Assess existing IT systems for quantum integration readiness. • Identify gaps (compute, networking, storage, security). • Plan procurement or retrofitting phases.
2. PREPARE RESOURCES	Build API and integration layers	• Develop or adopt APIs that interface with quantum algorithms and hardware. • Ensure compatibility with cloud-based and on-premises quantum resources. • Document integration architecture.
	Optimize resource and facility design	• Conduct energy consumption and power-supply analysis. • Identify retrofitting needs for hybrid (quantum + classical) environments. • Implement a monitoring system for resource performance.
3. ASSESS GOALS	Monitor enterprise quantum activity	• Track industry research, vendor roadmaps and competitor adoption. • Use trend reports to anticipate near-term opportunities.

	Maintain a comparison chart for outcomes	• Build a goals vs. capability comparison matrix. • Review quarterly to adjust timelines and investment focus. • Flag gaps between current and projected quantum capabilities.
4. RAISE WORKFORCE AWARENESS	Build foundational understanding	• Conduct organization-wide briefings on quantum benefits, risks and use cases. • Provide role-specific learning modules.
	Develop in-house expertise	• Launch training programs (physics, algorithm design, security, development). • Identify internal champions for cross-functional quantum initiatives. • Encourage collaboration between physicists, developers and domain experts.
5. PROMOTE DATA SECURITY & CRYPTO-AGILITY	Identify high-risk data	• Inventory all sensitive or regulated data sets. • Identify data vulnerable to "harvest now, decrypt later" threats.
	Implement quantum-resilient protections	• Conduct full encryption-use inventory across systems and applications. • Begin phased rollout of post-quantum cryptography (PQC). • Establish continuous crypto-agility procedures for future algorithm updates.