

Quantum-as-a-Service (QaaS)

What It Is, How It's Priced, and Contract Terms to De-Risk Adoption

Amanda Cline

Senior Counsel, Quadrant Law Group, LLP

Quantum-as-a-Service (QaaS) provides cloud-based, remote access to quantum computing resources, without the expense and complexity of owning or operating specialized quantum hardware. With the QaaS market concentrated among a handful of suppliers, negotiating fair contract terms can be a challenge. The nature of quantum output error presents new risks that are not contemplated under traditional SaaS contracts. Therefore, QaaS contracts should be structured to (i) define measurable service outcomes, (ii) preserve auditability/evidence, (iii) harden security and data-location controls, and (iv) ensure portability and orderly exit.

What is Quantum Computing?

Quantum computing uses quantum mechanics to solve complex problems faster than classical computers by processing qubits.¹ Qubits are “extremely fragile” and can lose their quantum properties due to interaction with environmental interference—noise—which can ruin a computation instantly.² Noise can also impact the accuracy of outputs, causing them to be more prone to error.

What is QaaS?

QaaS is a cloud delivery model that uses virtualization to host and deliver quantum resources through a supplier environment. Depending on the supplier, the service may include access to physical quantum hardware, emulated quantum processing units, quantum software applications, development environments, prebuilt algorithms, and other quantum tools and services, enabling teams to design locally and run/test workloads remotely on the supplier’s quantum computer.

Leading QaaS offerings are cloud platforms that provide remote access to quantum computers, often alongside simulators, SDK integrations, and hybrid quantum–classical tooling, without requiring organizations to host sensitive, specialized hardware. Key differentiators include managed cloud integration and developer tooling (Amazon Braket/Azure Quantum/IBM Quantum Platform/Google Quantum AI Cloud Services), open source frameworks (Google Cirq), high-availability and hybrid solver focus with onboarding support (D Wave Leap), broad SDK compatibility with direct access to a supplier’s QPUs (IonQ Quantum Cloud), and API-driven hybrid integration between classical infrastructure and QPUs (Rigetti Quantum Cloud Services).

QaaS Pricing Models and Cost Risk

Common pricing options include:

- Subscription plans to access quantum workspaces (often with tiered capabilities)
- On-demand / pay-as-you-go pricing (per task, per shot, per QPU-hour)
- Reserved/dedicated access to avoid shared scheduling queues.

¹ <https://aws.amazon.com/what-is/quantum-computing/>

² <https://www.ibm.com/quantum/blog/what-is-ftqc>

Commercial risk factors to consider include (i) resource availability/queuing delays due to limited quantum hardware bandwidth, (ii) capability gating behind higher subscription tiers or thresholds limiting experimentation, and (iii) usage-based spend ballooning as jobs get larger or more frequent.

QaaS Contract Considerations

In addition to assessing quantum fit and use cases, a business considering QaaS should involve its security, legal, and compliance teams early in the process, especially for regulated institutions. The following are six key focus areas for contract negotiations:

1. SLAs and Performance Remedies (beyond “three nines”)

Traditional SaaS service level agreements (SLAs) such as availability and response times are not necessarily fit-for-purpose when it comes to QaaS. Quantum-appropriate indicators that address problematic quantum processes and results can be negotiated, such as:

- Quantum fidelity - accuracy vs. expected result
- Quantum volume - overall capability metrics
- Queue availability / wait time (latency) for shared models
- Execution success rate - usable results per run

Remedies such as service credits, early termination without penalty, financial penalties proportionate to impact, and whether damages are subject to (or excluded from) standard liability caps should be explicit.

2. “Proof of Breach” Mechanics

Quantum outputs results can vary each time the algorithm is run. As such, demonstrating supplier breach may be difficult without agreed evidence. Imposing documentation and traceability requirements such as execution logs, time-stamped metrics, and incident reports, as well as ensuring the supplier has processes to respond to these requests is fundamental. For an organization, proof and documentation is the backbone for operational assurance, auditability, and dispute readiness in QaaS.

3. Liability

SaaS terms commonly cap liability at only a few months’ billing and exclude various loss categories. It is important to negotiate liability limits that reflect the economic value of the QaaS-enabled project, potentially with separate caps (or exclusion of caps) depending on the breach. It can be difficult to show quantum errors are the QaaS supplier’s fault as opposed to technological uncertainty without having an expert deep dive into each flawed result, and the downside exposure can be disproportionate to fees paid, especially where the use case supports critical R&D or sensitive risk sectors. If the contract contains a low cap and broad exclusions, the customer will bear most of the risk of loss, even where the supplier’s service or operations were deficient.

4. Data Security and Confidentiality

If QaaS is used in sectors such as finance, addressing data location and personal data processing at the outset is required to ensure compliance with data protection and privacy laws. Beyond standard confidentiality, organizations should evaluate specific security measures required to meet regulatory cybersecurity obligations.

5. Transition Services and Termination

Given market concentration and dependency risk, robust exit and termination terms should be negotiated in order to comply with regulatory requirements and internal policies, such as:

- retrieval of data in documented, interoperable formats;

- a right to data portability to other quantum or classical environments; and
- a support period sufficient to migrate without disruption.

The terms above should be negotiated with robust and clear transition services clauses to enable the organization to have cloud switching options available, which is also a requirement under the EU Data Act affecting cloud providers.

6. Regulatory Compliance and Export Controls

Quantum services are not subject to a bespoke regulatory regime, so contracts must address multiple regulatory angles, including:

- **GDPR and privacy laws:** define controller/processor roles and put DPAs in place where personal data is processed
- **Export controls:** allocate responsibility for compliance, including representations/warranties
- **Sector rules:** where the institution is subject to security obligations such as DORA and NIS 2, impose corresponding obligations on the supplier to support the institution's compliance
- **Regulatory adaptation clauses:** require good-faith renegotiation if regulatory change makes existing provisions incompatible with the system or its use

Conclusion

Adopting Quantum-as-a-Service can accelerate experimentation and reduce upfront infrastructure burdens, but the variability of its outputs and concentrated supplier market require contracts that are tailored beyond standard cloud terms. By negotiating quantum-appropriate performance metrics, robust "proof of breach" evidence rights, security and data-location controls, and clear portability/exit mechanics, organizations can de-risk spend, compliance exposure, and operational dependency while the technology matures.

For additional information, please contact:

Amanda Cline | Senior Counsel
Quadrant Law Group, LLP
T +1-949-396-1026
acline@quadrantlaw.com

This Bulletin is provided for informational and educational purposes only. It does not constitute legal advice or establish an attorney-client relationship. This Bulletin may be considered attorney advertising in some states.

Quadrant Law Group, LLP © 2026. All rights reserved.
203 N. La Salle St. Suite 2100, Chicago, IL 60601