Telefónica

Supplier assessment: readiness for the quantum era

Overview

The shift to post-quantum cryptography introduces new risks in managing technology suppliers. In Cloud environments and digital services, a significant part of the security posture depends on third parties not under direct control.

This questionnaire assesses providers' preparedness for quantum threats using technical, operational, and governance criteria. Its objective is to support decision-making in selection, procurement, and review processes.

The questions are organised by key domains and include priority levels for practical application.
All responses must include technical evidence to validate the information and ensure traceability.

See also: Assessing quantum readiness in Cloud providers: audit framework and technical questionnaire.

Summary

The following questionnaire is structured across four domains. Each question includes a priority rating:

- **CRITICAL** (must be answered before contracting or renewal).
- **HIGH** (must be addressed within the first 90 days).
- **MEDIUM** (important for programme maturity).

NOTE: This guide is indicative and may be adapted based on specific requirements and assessment objectives, taking into account aspects related to infrastructure, network architecture, security and applications.

All responses must be supported by appropriate technical evidence, ensuring proper traceability of the services within scope.

Domain 1: cryptography and algorithms What protects your data and how		
1	Cryptographic algorithms currently used for encryption in transit (TLS) and at rest, including the existence of a documented cryptographic inventory of the platform	**CRITICAL**
2	Existence of a formal roadmap for migration to post-quantum cryptography (PQC) algorithms (NIST PQC: ML-KEM, ML-DSA, SLH-DSA).	**CRITICAL**
3	Support or planned support for TLS 1.3 with post-quantum KEM extensions (hybrid key exchange).	**HIGH**
4	Evidence of crypto-agility assessment of the platform and defined frequency for cryptographic algorithm updates	**HIGH**
5	Key lengths currently in use and support for transitional mechanisms such as RSA-4096 or ECC P-384	**MEDIUM**

Domain 2: key and data management Who controls the keys and how		
1	Availability of customer-managed key models (BYOK / HYOK) and underlying HSM infrastructure.	**CRITICAL**
2	FIPS 140-3 certification status of HSM modules and roadmap for HSMs with native PQC support.	**CRITICAL**
3	Controls ensuring protection against “harvest now, decrypt later” (HNDL) scenarios, including cryptographic isolation between tenants.	**CRITICAL**
4	Policy for retention of encrypted data after contract termination and guarantees of cryptographic erasure.	**HIGH**
5	Availability of auditable logs covering all access to and use of cryptographic keys.	**MEDIUM**

Domain 3: operations and cryptographic resilience What happens when conditions change		
1	Existence of a documented response plan in the event of compromise of cryptographic algorithms currently in use.	CRITICAL
2	Defined SLA for updating or replacing cryptographic algorithms following vulnerability alerts issued by NIST or ENISA.	HIGH
3	Participation in standardisation initiatives or working groups related to post-quantum cryptography (e.g. ETSI QKD ISG, IETF, Cloud Security Alliance PQC).	HIGH
4	Execution of penetration testing focused on cryptographic infrastructure, including frequency and responsible parties.	MEDIUM
5	Customer notification processes for changes affecting cryptographic algorithms or protocols within the platform.	MEDIUM

Domain 4: governance and compliance Institutional commitment to the transition		
1	Availability (public or under NDA) of a formal readiness for the quantum era policy or PQC migration roadmap.	CRITICAL
2	Alignment with relevant European regulatory frameworks (NIS2, DORA, ENS) within the cryptographic strategy.	HIGH
3	Existence of contractual clauses ensuring timely cryptographic updates, or willingness to incorporate such clauses.	HIGH
4	Identification of a dedicated role or team responsible for managing the post-quantum transition.	MEDIUM
5	Availability of results from independent third-party cryptographic security audits for customer review.	MEDIUM

Scoring system for decision-making

To support supplier comparison or contract renewal decisions, a simple scoring model may be applied: 2 points for each CRITICAL item, 1 point for each HIGH item, and 0.5 points for each MEDIUM item.

The maximum possible score on this questionnaire is 16 points.

SCORE	CATEGORY	ACTION
>13	**Quantum-aware supplier** Demonstrates an active programme, supporting documentation and contractual readiness. **Proceed with negotiation of specific clauses.**	CONTRACT
8 - 12	**Supplier in transition** Demonstrates awareness but lacks a mature programme. **Require a roadmap with verifiable milestones as a contractual condition.**	CONDITIONAL
0 - 7	**Non-prepared supplier** Lacks awareness or a structured programme. **Represents a material risk for long-term data assets. Reassess or require binding commitments.**	REVIEW

About Telefónica Tech

Telefónica Tech is the leading company in digital transformation. It offers a wide range of integrated technological services and solutions in Cybersecurity, Cloud, IoT, Big Data, Artificial Intelligence and Blockchain.

telefonicatech.com