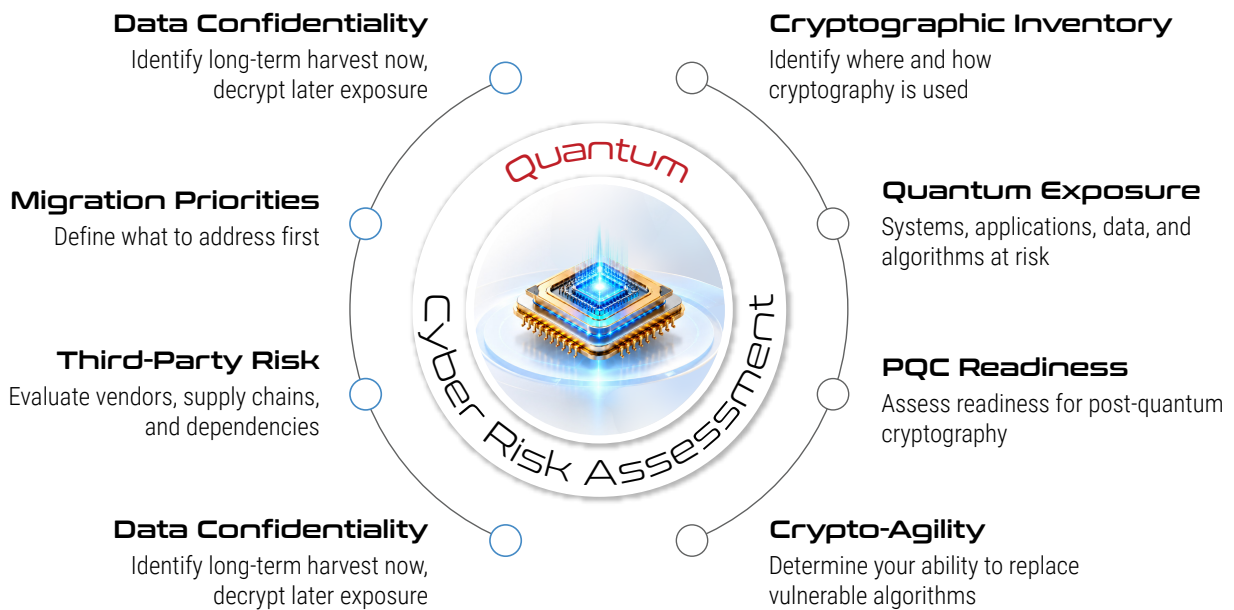


Is Your Encryption Ready for the Quantum Era?

Today's public-key cryptography protects your VPNs, TLS sessions, applications, and sensitive data. Quantum cyber risk assessment will eventually threaten these protections—and adversaries may already be harvesting encrypted data for future decryption.

Quantum Cyber Risk Readiness Assessment



Quantum Readiness Report



Cryptographic Risk Register

Prioritized quantum-related risks and exposures

PQC Migration Roadmap

Sequenced actions to improve quantum resilience



Executive Summary

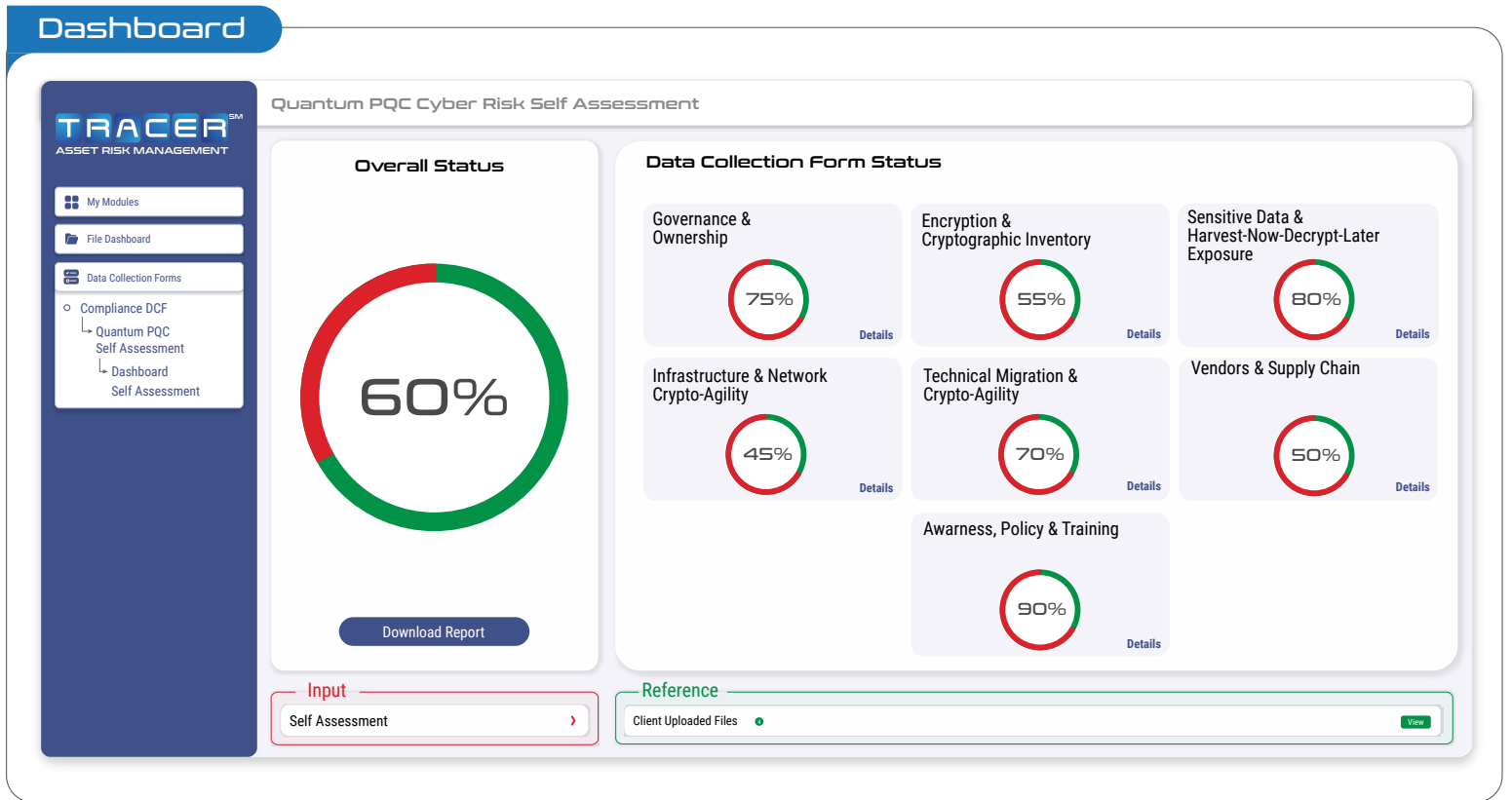
Leadership-ready findings and recommendations



Why Quantum Cyber Risk Matters?

- ✓ Establish a defensible quantum-readiness baseline
- ✓ Uncover cryptographic risk hidden in legacy and third-party systems
- ✓ Protect data requiring confidentiality beyond today's encryption lifecycle
- ✓ Turn quantum cyber risk into a prioritized, actionable program
- ✓ Prepare before customers, regulators, or auditors ask

Dashboard



Quantum Cyber Risk

Export

Governance & Ownership

0%

Governance & Ownership 5

Encryption & Cryptographic Inventory 5

Sensitive Data & Harvest-Now-Decrypt-Later Exposure 4

Infrastructure & Network Crypto-Agility 3

Technical Migration & Crypto-Agility 4

Vendors & Supply Chain 2

Awareness, Policy & Training 2

Governance & Ownership

Do you have a documented quantum-readiness or post-quantum cryptography (PQC) migration roadmap?

WHY THIS MATTERS
Independent surveys put 91% of security professionals with no formal PQC roadmap. A roadmap is the clearest single signal of readiness, and the first thing an auditor, regulator, or enterprise customer will ask to see.

Response

Yes

Partial

No

Not Sure

N/A

Status

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

25 Total Questions

Current Question	1
Not Answered	25
Answered Question(s)	0
Incomplete Question(s)	0

