GRC+ SERVICE SHEET · NOVEMBER 2026

Post-Quantum Cryptography Readiness Assessment

Financial supervisors now ask for quantum migration plans. MAS has consulted on migration timelines and the HKMA has published a transition toolkit. We find where you use cryptography, rank what is exposed and write the plan, with owners and milestones.

SERVICE
Advisory service

What It Is

We inventory where your systems use cryptography, rank what is exposed to quantum attack and write the migration plan your board and supervisor will ask for.

WHY IT MATTERS

You cannot migrate what you have not found

Most organisations have no full record of where they use cryptography. It sits in applications, libraries, devices and supplier products.
- Long-lived data exposed to harvest now, decrypt later
- Dependencies inside vendor products
- Supervisors starting to ask for plans and evidence

THE OUTCOME

A plan you can defend

Your management sees what is exposed, what moves first and who owns it.
- Evidence for your supervisor
- Procurement requirements for new systems
- A baseline you can keep current

What We Audit

Cryptographic inventory	Where you use encryption, signatures and key exchange: algorithms, key lengths, protocols, certificates and the systems they support.
Exposure and priority	Which data must stay confidential for years, which systems are hardest to change, and what to move first.
Vendors and procurement	Supplier migration roadmaps, and whether new purchases support quantum-safe algorithms or can be upgraded to them.
Plan and governance	Owners, milestones and reporting, compared with what your supervisor has published.

What You Receive

The readiness report and migration plan PDF	Each gap with its evidence, its risk, the requirement concerned and what to change.
A management summary In the report	Where you stand, the main risks and the decisions needed.
A walkthrough Video call	A session with your team to go through the findings and answer questions.

From Scope to Report

1	**Scoping** Entities, activities, requirements and samples in scope, agreed in writing.
2	**Inventory** Documents, scans and interviews to find where cryptography is used.
3	**Analysis** Exposure ranked by data lifetime and system, and supplier roadmaps checked.
4	**Draft findings** You see every conclusion before it is final and can add evidence.
5	**Report** The report for your management, with each gap, its risk and what to change.

A guide, not a fixed promise: the length of each phase depends on your scope and on how quickly evidence and people are available.

Regulations That Ask for It

MAS TRM (Singapore)	
NIST IR 8547 (United States)	We inventory where your systems use cryptography, rank what is exposed to quantum attack and write the migration plan your board and supervisor will ask for.
SAMA Quantum Circular (Saudi Arabia)	

Why Organisations Choose GRC+

We follow changes to the requirements	We track regulators in your markets, so the work starts from the current text.
Independent of your suppliers	We take no margin on a product we assess or recommend.
Tested, not only read	We test what happens in your records and systems, not only what your documents say.
Written scope first	You agree the scope and the fee before any work starts.

Questions Buyers Ask

Do we have to replace our cryptography now?

No. The first steps are the inventory, the ranking and new procurement requirements. The dates depend on your supervisor and your own estate, and we set them out in the plan.

Does this replace our security architecture work?

No. It gives your architects the inventory and priorities they need. We also run security architecture risk assessments if you want them together.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/post-quantum-cryptography-readiness-assessment