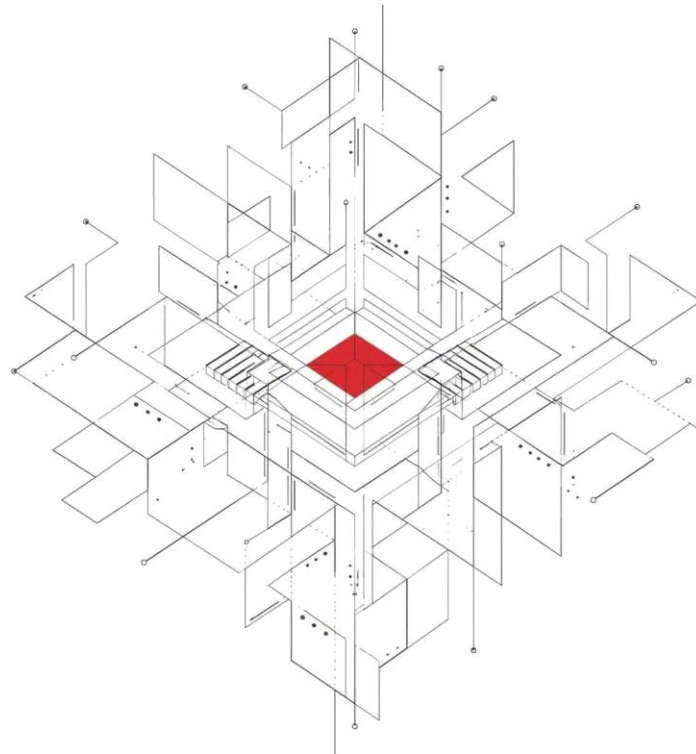


SINGAPORE PUBLISHED TWO QUANTUM DOCUMENTS ON THE SAME DAY.



Both documents are advisory, yet the Handbook still sets dated requirements for CII owners.

Both state they are "not mandatory, prescriptive nor exhaustive" (Handbook p.3, Index p.3).

Sources: CSA Quantum-Safe Migration Handbook v1 and Quantum Readiness Index v1.0, both 16 Jul 2026



A HANDBOOK AND A SELF-ASSESSMENT, NOT A REGULATION

The Handbook sets out what is at stake and what CSA says organisations should do. The Index assesses where an organisation sits on organisational readiness, not whether cryptographic migration has occurred.

Both carry the same disclaimer: "not mandatory, prescriptive nor exhaustive" (Handbook p.3, Index p.3).

Both run on the same five domains: Risk Assessment, Governance, Technology, Training and Capability, External Engagements.

Both documents run on the same five domains.

RISK

GOVERNANCE

TECHNOLOGY

TRAINING

EXTERNAL



ADVISORY TEXT CARRYING DATED CII REQUIREMENTS

Handbook p.25 is the only place either document sets fixed dates. CSA addresses them to CII owners.

31 MAR 2027

CII owner's quantum-safe migration plan submitted to CSA

1 JAN 2028

New CII systems with a digital component should support quantum-safe algorithms or be quantum-safe ready

31 DEC 2031

Migration across CII systems complete. Vulnerable cryptography should no longer be used

CSA states detailed guidance to support CII owners is still being developed (p.25). The Handbook does not state that these dates are legally enforceable.



READ THE LANGUAGE. IT IS NOT ALL THE SAME.

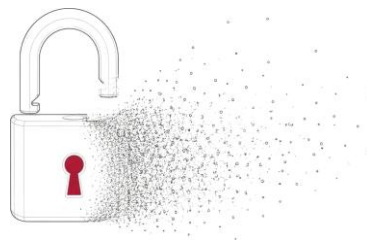
MUST: organisations "must start now with planning" (p.4).

SHOULD: public-key cryptography vulnerable to Shor "should be prioritized for replacement" (p.7).

SHOULD: procurement policies should be updated to "explicitly require" crypto-agility and vendor post-quantum roadmaps (p.23).

DEPRECATED: RSA, DH and ECC are identified as deprecated in the Handbook's algorithm table (p.26).

The language establishes different levels of expectation. It does not, by itself, establish legal enforceability. Inventory, threat modelling and testing are presented as recommendations or guidance unless the Handbook explicitly states otherwise.

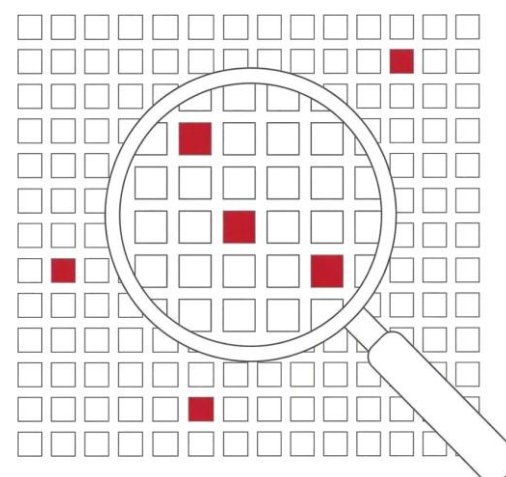


SCOPE DOWN FIRST, THEN DISCOVER

The no-regret move is narrow: identify your most critical systems and run cryptographic discovery on those first (p.12, p.14).

Start with artefacts you already hold. HSM and key management logs, certificate systems, server configurations, network diagrams (p.15).

CSA states automated discovery tools are "still maturing" and will "not catch everything" (p.15 to 16).



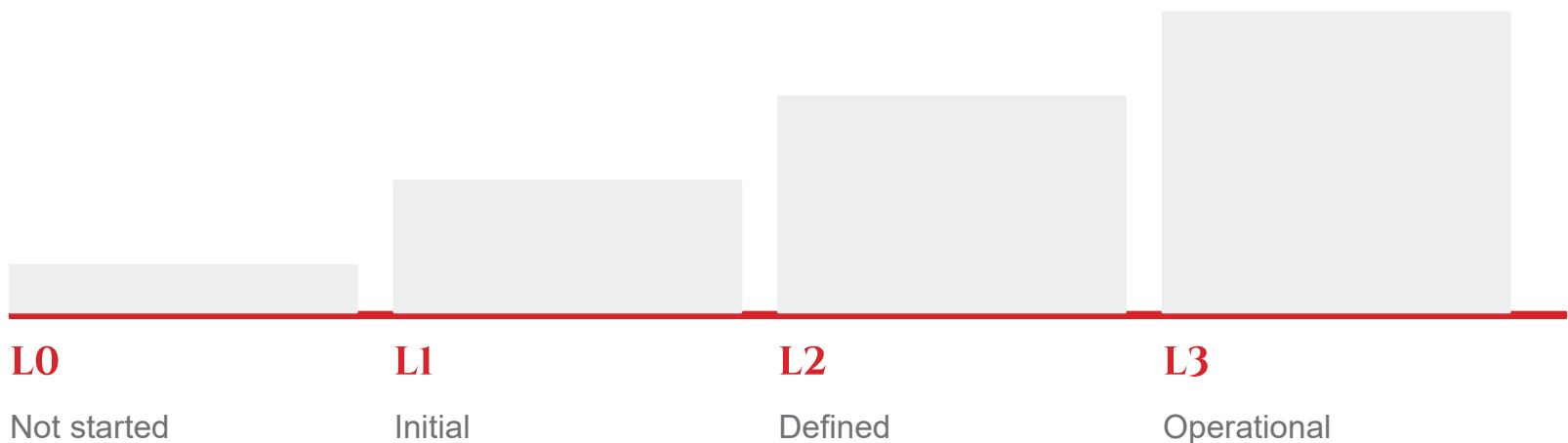
It goes past inventory. The Handbook says cryptographic policy should "maintain a live cryptography inventory", and that vendors should supply a Cryptographic Bill of Materials, CBOM (p.24, p.38).

READINESS IS NOT MIGRATION

A self-assessment at go.gov.sg/qri. You answer, a readiness level is computed per objective, and a PDF report is returned to you (p.9, p.12).

Five domains, two objectives each, and four maturity levels. The first objective in every domain is the "no-regrets" starting point (p.10, p.11).

The Index defines readiness as "the organisational processes and expertise required to plan and execute the migration" (p.8). It assesses organisational readiness, not proof that cryptographic migration has occurred.



WHAT THE INDEX DOES, AND WHAT IT DOES NOT

THE QRI SITS WITHIN AN EXISTING FIELD OF QUANTUM-READINESS ASSESSMENT MODELS.

Its reference list cites seventeen prior works, including WEF, Accenture, HAPKIDO, evolutionQ, Deloitte and FS-ISAC (p.14).

The QRI is a self-assessment. The Index does not require external verification or submission to CSA (p.8, p.12).

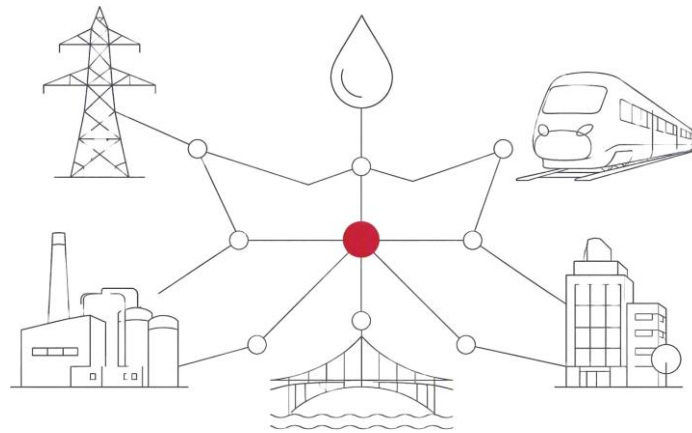
Results are returned to the respondent as a PDF report. The Index "does not prescribe specific solutions or minimum levels of readiness" (p.8).

It measures organisational process and expertise, not cryptography in production.

SITG-Consulting interpretation: an organisation could reach L3 without having migrated a single system.



CII OWNERS ARE ON A DIFFERENT FOOTING



The dated milestones identified in the Handbook apply to CII owners (p.25). No other category is given dates.

Sectors named as most exposed to Harvest-Now-Decrypt-Later: energy, water, transport, finance, healthcare, government (p.8).

From 1 Jan 2028, new CII systems with a digital component should support quantum-safe algorithms or be quantum-safe ready (p.25).

SITG-Consulting interpretation: non-CII organisations inherit the strategic direction, but these documents do not assign them the CII dates.

WHAT MAKES THIS MORE THAN AWARENESS MATERIAL

DATES

Dated CII milestones, with CSA named as the recipient of the plan (Handbook p.25).

DEPRECATION

A published algorithm table identifying RSA, DH and ECC as deprecated (p.26).

DECISION RIGHTS

A four-stage RACI across steering committee, CISO, CIO and business owner (p.22 to 23).

WORKED THREATS

Hospital VPN and family office, via STRIDE-LM and MITRE ATT&CK (p.16 to 20).

CANDOUR

CSA records scepticism about the scale of Harvest-Now-Decrypt-Later and the maturity of QKD testing standards (p.8, p.28).



THE GAPS ARE REAL, AND THEY MATTER

No CBOM specification. Organisations are told to request one from vendors, with no format or minimum content defined.

No definition of "quantum-safe ready", the phrase carrying the 1 Jan 2028 procurement expectation.

No funding model, no quantitative risk methodology, no reference migration architecture.

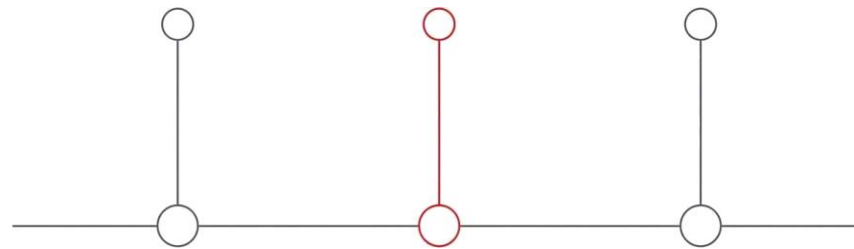
No assurance model. Validation covers five areas (Handbook p.32 to 33), but no evidence standard, audit expectation or enforcement mechanism is stated.

The Index prescribes no minimum level, requires no external verification, and does not require submission of the result to CSA (Index p.8, p.12).

Neither document states a linkage between an Index result and the CII migration plan due 31 Mar 2027.



WHAT CHANGES NOW



CII owners: the Handbook sets a plan to CSA by 31 Mar 2027 and migration complete by 31 Dec 2031. Work back from those dates (p.25).

For non-CII organisations, these documents do not assign the CII migration dates as general deadlines.

SITG-Consulting interpretation: procurement and supplier requirements are likely to become an important transmission mechanism for non-CII organisations.

Run the Index for a baseline, and do not mistake a readiness score for migration progress.

Four practical moves: name accountability, scope your crown jewels, discover the cryptography in those systems, ask vendors for their roadmaps (p.12 to 13).

SITG-CONSULTING OPINION

SINGAPORE HAS SET THE CLOCK. IT HAS NOT SET THE METHOD.

Treat the CII dates as fixed planning constraints. They are the only dated points either document sets.

Plan for evidence, not merely a readiness score. Neither document defines an evidence standard, so decide now what proof you would put in front of a regulator or a board.

Treat procurement and supplier management as important pressure points.

Design for algorithm change. Standards and acceptable algorithms will evolve.

BRIAN COUZENS

brian.couzens@sitg-consulting.com sitg-consulting.com

Turning the Singapore requirements into an evidence-backed migration plan? Get in touch.

Not a CSA statement. Based on Quantum-Safe Migration Handbook v1 and Quantum Readiness Index v1.0.

© 2026 SITG-Consulting. All rights reserved.

