SafeCipher
safecipher.com

PREPARING for POST-QUANTUM CRYPTOGRAPHY

THE 2026 CRYPTO COMPLIANCE CLOCKS

3 deadlines + 2 mandates that will redefine cryptography — and what to do now to avoid outages, audit pain, and procurement blockers.

SafeCipher | safecipher.co.uk | Vendor-neutral PQC, PKI, HSM and crypto agility specialists

2026 isn't "the year PQC arrives". It's the year the compliance clocks start forcing cryptography change.

Three clocks matter immediately:

- 15 March 2026: Public TLS certificates drop to 200 days.
- 21 September 2026: FIPS 140-2 moves to "Historical".
- 2026: CNSA 2.0 expectations start landing in network equipment.

If you're not automating certificates, don't have a full view of where cryptography is used, and don't have a plan for PQC and FIPS changes, the result will be outages, audit headaches, or blocked purchases.

CLOCK #1 (15 MAR 2026): TLS CERTS DROP TO 200 DAYS

- More renewals, more change events, more failure points.
- Manual processes don't survive higher renewal frequency.
- Miss one renewal = outage + incident + customer impact.

What to do now:

- Discover every certificate, endpoint, and owner (including "unknown unknowns").
- Automate issuance, renewal, deployment, and monitoring with alerting and rollback.
- Define ownership and change controls so renewals don't depend on one person.

CLOCK #2 (21 SEP 2026): FIPS 140-2 ENDS FOR NEW SYSTEMS

- FIPS 140-2 validations increasingly won't satisfy new systems/new procurements in federal-aligned contexts.
- Vendors may lag; "we assumed it was FIPS" becomes a contract and audit problem.
- HSM/KMS/library choices can quietly become non-compliant.

What to do now:

- Inventory where FIPS-validated crypto is relied upon (HSMs, KMS, appliances, libraries).
- Verify vendor claims against CMVP listings and identify replacement paths.
- Plan upgrades to FIPS 140-3 modules with testing windows and fallback options.

CLOCK #3 (2026): CNSA 2.0 HITS NETWORKS (HYBRID/PQC)

- VPNs/routers and gateways begin aligning to CNSA 2.0 expectations.
- Hybrid changes can expose interoperability problems across suppliers.
- Handshake size and performance edge cases appear in real-world networks.

What to do now:

- Run interoperability testing across clients, gateways, load balancers, proxies, and inspection tooling.
- Define a phased hybrid strategy (where to enable first, where to hold).
- Adopt crypto agility patterns so algorithms can be swapped without re-platforming.

CLOCK #4: NO INVENTORY = NO COMPLIANCE

- RSA/ECC hides in code, appliances, cloud services, HSM policy, and devices.
- You need owners, lifecycles, dependencies, and “where it breaks” mapped.
- This becomes your evidence base for PQC and FIPS transition.

What to do now:

- Build a cryptographic inventory (algorithms, locations, owners, lifecycles, dependencies).
- Prioritise by business criticality and data lifespan (long-lived confidentiality first).
- Turn the inventory into a roadmap with milestones and measurable progress.

CLOCK #5 (2030, STARTS NOW): RSA-2048 BECOMES LEGACY

- NIST signals RSA-2048 becomes legacy after 2030.
- Large estates have thousands of apps, appliances, and peripherals with RSA-2048 baked in.
- Waiting pushes you into a 2029–2030 fire drill and compliance exceptions.

What to do now:

- Identify where RSA-2048 is used today and which systems can’t be upgraded easily.
- Collect vendor roadmaps now; require stronger baselines (e.g., RSA-3072+) in new procurements.
- Pilot migration paths early (uplift + hybrid readiness) to avoid a late, high-risk cutover.

Call to action

- Comment “CLOCKS” and we’ll send the SafeCipher 2026 Readiness Checklist.
- Or DM for a readiness scan / roadmap session tailored to your estate.