The certificate estate nobody can see.

And the March 2027 deadline that exposes it.

Certificate lifetimes are being cut in phases, and the next cut is the one that breaks manual processes. You cannot protect what you have never inventoried - and many organisations do not know how many certificates they hold or where they are deployed.

100 days

Maximum public TLS validity from 15 March 2027

10 to 11

Different certificate authorities in a typical estate, plus self-signed certificates nobody tracks

81%

Certificate-related outages linked to expired or misconfigured certificates

THE DEADLINE IS VISIBLE.
THE FULL CERTIFICATE ESTATE OFTEN IS NOT.

MARCH 2027 IS THE CHANGE THAT ACTUALLY HURTS

In April 2025, the CA/Browser Forum approved a phased reduction in public TLS certificate lifetimes. The 200-day cut is already in force and many estates absorbed it without much drama. The next one is different: at 100 days, renewal stops being an annual task and becomes a quarterly operation. That is the point at which spreadsheets, calendar reminders and tribal knowledge stop working reliably - and it is close enough that planning has to start now.

BEFORE MARCH 2026	NOW	15 MARCH 2027	15 MARCH 2029
398 days The old annual world, managed on a spreadsheet.	**200 days** In force now and largely absorbed.	**100 days** Quarterly renewals become the floor. This is the change to plan for.	**47 days** Plus domain revalidation every 10 days. The destination, not the immediate deadline.

THE OPERATIONAL CLIFF

From March 2027, renewals move from annual to quarterly per certificate, heading towards eight or more a year by 2029.

Manual tracking becomes fragile, and a missed renewal can become an outage on a customer-facing service.

Every process designed around an annual cycle has to be reviewed.

THE VISIBILITY GAP

Large enterprises can run 140,000 or more internal certificates with limited central oversight.

Estates may span ten or eleven certificate authorities, as well as self-signed certificates issued outside the normal process.

The certificates nobody inventoried are the ones most likely to expire silently.

Discovery gaps are the first risk to close - because an unknown certificate cannot be governed by any process or platform.

DISCOVERY, NOT DATA ENTRY. AND DELIBERATELY NOT A CLM.

A certificate lifecycle management platform only knows what it has been told about. Feed it an incomplete list and it manages an incomplete estate, while the certificates most likely to cause outages are often the ones nobody registered. Certificate discovery starts from the estate itself, not a manually supplied spreadsheet.

ONE DOMAIN. THE ESTATE AS IT ACTUALLY EXISTS.
Provide ITB with a single domain and the health check discovers the certificate estate as it actually exists. No imports, nothing to deploy and no long, resource-heavy implementation project.

WHAT YOU HAVE

Certificates across public, private, third-party and self-signed sources.

Certificate Transparency data can highlight rogue or unexpected issuance associated with your domains.

WHERE IT LIVES

Host and endpoint-level mapping, including network, cloud, DNS and registrar assets.

Active deployments can be separated from unused or historical records.

HOW IT IS USED

Expiry, issuer, key strength, algorithm and configuration by certificate and endpoint.

Weak, unexpected or exposed deployments surface before they become an incident.

THE OUTCOME

A clear point-in-time report of the visible certificate estate: deployments, issuers, expiry dates, configuration weaknesses and the risks that need attention first.

WHAT IT DOES NOT DO

The health check does not issue, renew, revoke or deploy certificates. It is not a CLM and does not replace one. Remediation and lifecycle decisions remain with your chosen tools and operating model.

POST-QUANTUM READINESS STARTS WITH AN INVENTORY, NOT A MIGRATION

Harvest-now-decrypt-later is a current risk, not just a future scenario: encrypted traffic captured today may be stored and decrypted once sufficiently capable quantum computing exists. That makes long-lived confidential data relevant now. The migration itself will take years. The first step is simply knowing which hosts and endpoints still rely on quantum-vulnerable cryptography.

2030	2035
NIST transition guidance begins deprecating quantum-vulnerable public-key algorithms for many uses.	NIST transition guidance moves to disallow those algorithms across the relevant uses.

WHAT THE HEALTH CHECK SHOULD REVEAL

- ✓ A current inventory built from discovery rather than a manually supplied list.
- ✓ The hosts and endpoints presenting each certificate, including active versus unused deployments.
- ✓ Issuers, expiry dates, key strength, algorithms and configuration weaknesses.
- ✓ Unexpected or potentially rogue certificate issuance linked to your domains.

Start with the certificate health check.

ITB can help you reveal the certificate estate as it exists today: what you hold, where it is deployed, what expires when and which cryptographic risks need attention. The result is visibility and evidence - not another lifecycle management platform.

Talk to ITB | it-b.co.uk/contact