

AUSTRALIAN GOVERNMENT & PARTNERS · EXECUTIVE BRIEFING

# The Certificate Deadline Is Already Here

What the global shift to short-lived TLS certificates means for your agency — and what to do about it

---

# The Rules Changed. The Clock Is Already Running.

47

DAYS

Maximum cert lifetime  
by March 2029

200

DAYS

Maximum cert lifetime  
**in force since 15 March 2026**

398

DAYS

What most agencies  
are still managing to

**CA/Browser Forum Ballot SC-081 passed 11 April 2025.** Apple proposed 47 days. Google voted yes immediately. This is ratified industry policy — enforced by browser vendors through trust store inclusion. No certificate lifetime reduction has ever been reversed once passed.

# What This Means for Your Agency

TLS certificates are the padlocks on every government website, API, and digital service. When they expire, citizens are blocked. When they're mismanaged, systems break.



## Manual renewal breaks down

Many agencies have historically relied on annual manual renewal, aligned to the previous 398-day maximum. At 200 days — and eventually 47 days — that process becomes operationally impossible across hundreds of systems.



## Legacy infrastructure is exposed

Load balancers, firewalls, and on-premises appliances common in government don't support modern certificate automation. Upgrading them requires procurement cycles measured in months.



## Compliance risk is real

ASD ISM controls address certificate lifecycle management. Manual renewal workflows at this cadence introduce availability and configuration risks inconsistent with Essential Eight resilience expectations and PSPF governance obligations.

# The Cost of Doing Nothing

## WHEN A CERTIFICATE EXPIRES



### Citizens are blocked

Chrome, Edge, and Safari display a full-page security warning. Most citizens will not proceed — they cannot access the service.



### Systems cascade

Inter-agency APIs, federated identity, and shared services connections fail — often silently, often across multiple systems simultaneously.



### It becomes public

Government website outages from expired certificates are publicly visible and frequently reported. They undermine citizen trust in digital government.

### REAL-WORLD PRECEDENT

"During the 2018–19 US government shutdown, more than 80 federal websites went offline — not from a cyberattack, but because furloughed staff couldn't manually renew certificates. Any environment where renewal depends on a named individual rather than an automated process carries the same structural risk."

### THE TIMELINE IS ACCELERATING

200 days maximum	Active now ✓
100 days maximum	March 2027
47 days maximum	March 2029

# There Is a Better Path

Cloudflare sits in front of your existing infrastructure and handles certificate management automatically — without replacing a single system, without moving your DNS, and without a lengthy procurement cycle.

## PROTECT NOW

### Weeks, not months

Cloudflare proxies your public-facing services and takes over certificate issuance and renewal at the edge. Your origin systems are untouched. Citizens always see a valid certificate.

## NO DNS MIGRATION

### Keep your existing infrastructure

For agencies that cannot migrate DNS, Cloudflare's partial setup allows proxying via a CNAME record per hostname — no DNS migration required. Agencies that can delegate DNS to Cloudflare benefit from fully automated certificate management.

## MODERNISE AT YOUR PACE

### A stable platform for the long term

Cloudflare acts as the stable intermediary while you modernise origin systems on your own timeline — 12, 24, or 36 months. The deadline pressure is removed from day one.

# Why Cloudflare

✓ **IRAP assessed**

Cloudflare has completed an IRAP assessment. Contact us for current scope and applicable workload classifications under the PSPF.

✓ **Australian PoPs — including Perth**

Cloudflare operates in Sydney, Melbourne, Perth, Brisbane, and Canberra. Traffic stays in-country where required.

✓ **Already managing certificates at scale**

Cloudflare automatically manages certificates for millions of domains globally. More than 22% of all websites sit behind Cloudflare's network (W3Techs, May 2026).

✓ **ISO 27001 · SOC 2 Type II**

Independently audited security controls. Compliance documentation available via the Cloudflare Trust Hub.

FORRESTER TOTAL ECONOMIC IMPACT · JANUARY 2026

**227%**

Return on investment

**<6 mo**

Payback period

**35%**

IT ops time reduction

Source: Forrester TEI of Cloudflare, January 2026. 35% = reduction in IT ops time for certificate and DNS management. [tef.forrester.com/go/cloudflare/cloudflaretei/](https://tef.forrester.com/go/cloudflare/cloudflaretei/)

ONE CONVERSATION. THREE OUTCOMES.

# Let us show you where your agency stands — and what it takes to get ahead of this.



## Certificate Inventory Audit

Understand your current exposure — how many certs, when they expire, which systems are at risk.



## 30-Minute Architecture Review

Walk through how Cloudflare fits in front of your existing infrastructure — no commitment required.



## Roadmap to Compliance

A phased plan that gets you protected immediately and modernised on a timeline that fits your procurement cycle.

