Measuring Certificate Management Maturity
in Your Organization

Most organizations have an intuitive sense of whether their certificate management is in good shape or barely holding together, but intuition is a poor basis for prioritizing investment or demonstrating progress to leadership. This article offers a structured way to actually measure certificate management maturity, giving organizations a concrete way to assess where they stand and what improvement would actually look like.

Level One: Reactive and Undocumented

At the least mature level, certificate management happens purely reactively: certificates are requested and installed as immediate needs arise, no central inventory exists, renewal depends entirely on individual memory or informal calendar reminders, and incidents are discovered only when something actually breaks. Organizations at this level typically have no clear answer to how many certificates they actually have in production, and outages are treated as isolated, surprising events rather than predictable outcomes of a known process gap.

Level Two: Documented but Still Largely Manual

Organizations at this level have taken the first meaningful step of building a certificate inventory and documenting basic processes, but renewal and issuance still happen largely manually, with automation limited to isolated scripts covering a subset of the environment rather than comprehensive coverage. Monitoring may exist but often depends on someone actively checking a dashboard rather than genuinely proactive alerting, and certificate-related incidents, while less frequent than at level one, still occur with some regularity.

Level Three: Automated for the Common Case

At this level, the bulk of routine certificate issuance and renewal is automated through ACME or a CLM platform, discussed throughout this series, monitoring includes proactive alerting well ahead of expiration, and a documented incident response process exists for the less common cases automation does not fully cover, such as revocation during a genuine compromise. Organizations here have largely eliminated routine expiration-related outages, though edge cases and less common certificate categories, such as network appliances or specialized machine identities, may still lag behind the primary automation coverage.

Level Four: Comprehensive Automation With Strong Governance

Mature organizations at this level have extended automation and monitoring across essentially their entire certificate estate, including machine and AI identities, IoT devices, and network infrastructure, paired with strong governance: documented policy, regular audits, tested incident response and resilience procedures, and clear ownership for every certificate category. Organizations here are well positioned for the shrinking certificate lifetime schedule discussed throughout this series, since their existing automation and governance already anticipate the operational demands that schedule requires.

Level Five: Continuously Optimized and Forward-Looking

The most mature organizations treat certificate management as a continuously improving discipline rather than a solved problem, actively tracking industry developments such as post-quantum readiness and format changes discussed elsewhere in this series, running regular maturity self-assessments, and proactively adjusting their strategy ahead of industry deadlines rather than reacting to them once they take effect. This level is genuinely rare, but it represents the practical ceiling worth aiming toward for organizations with meaningfully complex or high-stakes certificate estates.

Using a Maturity Model to Prioritize Investment

Honestly assessing an organization's current maturity level against this framework gives a concrete basis for prioritizing where investment should go next, since the right next step differs considerably depending on starting point: an organization at level one needs basic inventory and documentation before automation investment makes sense, while an organization already at level three benefits more from extending automation's reach than from further automating what is already well covered.

Where AI and Machine Identity Coverage Fits Into Maturity Scoring

A genuinely honest maturity assessment today needs to specifically evaluate how well an organization's certificate management extends to machine and AI identities, discussed throughout this series, since many organizations that would otherwise score at level three or four for their traditional web-facing certificates are considerably less mature when it comes to the rapidly growing population of AI agent and automated service certificates, a gap worth surfacing explicitly rather than allowing strong traditional certificate practices to mask a genuine blind spot in this newer, fast-growing category.

The Countdown Is Already Running: 200 Days, 100 Days, 47 Days

Every certificate conversation in 2026 eventually arrives at the same clock, and it is worth closing on it here. The CA/Browser Forum's Ballot SC-081v3 is not a proposal under discussion; it is an approved, already-in-motion schedule. Maximum public TLS certificate lifetimes fall from 398 days to 200 days on March 15, 2026. They fall again to 100 days on March 15, 2027. By March 15, 2029, they drop to just 47 days, with domain validation itself needing to be re-proven roughly every 10 days.

01

Translate that into operational terms and the picture gets stark quickly. An organization currently renewing certificates a few times a year will be handling renewal events on the order of every couple of weeks by the end of this countdown, across every endpoint it operates. Manual tracking, calendar reminders, and a spreadsheet somebody checks once a month will not survive contact with that cadence. What has always been an occasional chore is becoming a continuous, automated operation, whether an organization plans for it or not.

02

Organizations scoring at level one or two on this maturity model are in a genuinely urgent position given the schedule below, since the gap between their current manual processes and the automation required to survive renewals every 47 days is considerably larger than it is for organizations already operating at level three or above.

03

The 200-day, 100-day, and 47-day milestones are not distant hypotheticals; the first has already arrived. Organizations that build the automation loop now, generating keys, vaulting them securely, brokering issuance across Certificate Authorities through APIs, and rebinding certificates to live endpoints without manual intervention, will meet each deadline without disruption. Organizations that wait will be rebuilding their certificate operations under deadline pressure, with far less room for error and far less time to get it right. The countdown is the call to action. The only real decision left is whether to automate on your own schedule, or on the CA/Browser Forum's.