47-Day Certificate Automation Readiness Checklist

CYBERARK

CHECKLIST

A practical benchmark to guide your transition to short-lived TLS certificate automation

Public TLS certificates are changing. In a phased approach starting in 2026, their maximum validity will drop to 200 days. Shorter limits, 100 days and eventually 47 days, will follow. This change will force monthly renewal for teams that haven't aligned certificate operations with change control (i.e., maintenance windows and operational approval processes). Organizations will see an 8-12x increase in the renewal rate, which is almost certain to break manual workflows and overload unprepared teams.

Use this checklist to guide your transition to short-lived TLS certificate automation.

Step 1: Discover and Assess Public TLS Certificates

- [ ] Continuously discover all public TLS certificates with automated scanning.
- [ ] Categorize certificates by environment, risk, business impact, and ownership.
- [ ] Identify shadow certificates and unauthorized CAs.
- [ ] Align expiring certificates to change windows.

Step 2: Assign Ownership and Enforce Lifecycle Policy

- [ ] Define ownership by team or platform. Establish group-based accountability.
- [ ] Create issuing templates per CA; enforce global CA/B Forum-aligned validity rules.
- [ ] Set and enforce policies for validity, renewal windows, and exceptions.
- [ ] Configure SLA alerts and escalation paths.

Use certificate data to forecast impact by phase and prioritize remediation.

- **PHASE 1:** 200-day certs by March 2026
- **PHASE 2:** 100-day certs by March 2027
- **PHASE 3:** 47-day certs by March 2029

BEST PRACTICE:

Target automation coverage of at least

95%

of public TLS certificates, then close the remaining 5% through phased expansion to achieve full 100% renewal automation.

Step 3: Automate Renewal at Scale

- [ ] Prioritize automating key systems; expand iteratively.
- [ ] Configure auto-renewal per issuing template; validate readiness per CA.
- [ ] Verify that automation spans clouds, platforms, and tools.
- [ ] Ensure CA or algorithm changes can be executed without outages.

BEST PRACTICE:

Ensure renewals generate new keys every cycle, reducing compromise risk.

Step 4: Monitor and Prove Control

- [ ] Show expiration risk, SLA adherence, and automation coverage via dashboards.
- [ ] Track Phase 1–3 impacted certificates by CA and endpoint.
- [ ] Ensure renewal success rate exceeds 99%, with <1 hour time-to-remediation.
- [ ] Deliver monthly certificate posture and CA/B compliance reports to executives, demonstrating audit readiness.

This checklist provides a technical benchmark for navigating the shift to short-lived TLS certificates, but it's just the beginning. To fully prepare for 47-day renewal cycles, organizations need a comprehensive, phased strategy that aligns discovery, ownership, automation, and monitoring. **CyberArk's 47-Day Automation Playbook** expands on each step with detailed execution guidance, a certificate automation maturity model, and suggested KPIs — giving security, infrastructure, and platform teams a clear path to scalable, audit-ready certificate automation.

Download the playbook to get an end-to-end strategy for TLS certificate automation and ensure your team is ready for what's next.

CYBERARK® | MajorKey