

47-Day Readiness Audit Checklist

82-point self-audit: what breaks in your environment when certificate velocity increases 8x?
CA/Browser Forum Ballot SC-081v3 · TLS validity drops to 47 days by March 2029

FIXMYCERT.COM

How to use this checklist: work through each section and check every item you can prove today — not what's planned or promised. Your score = checked items ÷ 82. Re-run quarterly through March 2029. Phase 1 (200-day validity) took effect March 15, 2026; Phase 3 (47 days + 10-day DCV reuse) arrives March 15, 2029.

Quick reference: (1) Know every public TLS cert you own, who renews it, and whether renewal is automated end-to-end. (2) Test at 2x velocity now; fix what breaks before 8x arrives. (3) The 10-day DCV reuse limit in Phase 3 is harder than the 47-day validity — plan DNS-01 automation first. (4) If any renewal requires a human clicking something, that's your #1 risk.

1. Scope & Inventory Audit

Objective: Confirm you know exactly how many publicly-trusted TLS certificates you own and where they live.

- | | |
|--------------------------|--|
| ☐ | Complete inventory of all publicly-trusted TLS certificates exists |
| ☐ | Inventory includes issuing CA, expiration date, key algorithm, and SAN list for each cert |
| ☐ | Inventory covers ALL environments: production, staging, DR, dev, test |
| ☐ | Inventory includes CDN-managed certificates (Cloudflare, AWS CloudFront, Akamai, Fastly) |
| ☐ | Inventory includes load balancer certificates (F5, HAProxy, Nginx, ALB/NLB) |
| ☐ | Inventory includes certificates in container orchestration (Kubernetes cert-manager, service mesh) |
| ☐ | Inventory includes certificates provisioned by developers outside central IT |
| ☐ | Inventory distinguishes public TLS from private/internal PKI (only public is affected by SC-081v3) |
| ☐ | Certificate Transparency logs (crt.sh) checked for certificates not in your inventory |
| ☐ | Total count of public TLS certificates documented |
| ☐ | Estimated renewals per year at 47-day validity calculated (count × ~8) |

■ Shadow certificates are the #1 discovery gap. Developer-provisioned Let's Encrypt certs in CI/CD won't show up in your CLM unless discovery covers those environments. CT logs are the truth source for public certs.

2. Renewal Ownership Audit

Objective: For every certificate, confirm there is a defined owner and a defined renewal method — manual or automated.

- | | |
|--------------------------|--|
| ☐ | Every certificate has an assigned owner (person or team, not "IT") |
| ☐ | Ownership is documented in your inventory/CMDB, not just tribal knowledge |
| ☐ | Each certificate's renewal method is classified: Fully Automated / Semi-Automated / Manual |

☐	Percentage of certificates that are fully automated (no human in the loop) documented
☐	Percentage requiring manual steps (DCV approval, file placement, ticket) documented
☐	Manual renewal certificates identified as migration candidates
☐	Certificates with single-person dependencies identified (bus factor = 1)
☐	Renewal responsibility survives employee turnover (documented, not in someone's head)

■ “Semi-automated” means “manual” when it matters. If a human has to click approve at 3 AM on a weekend, it's manual. The honest enterprise split is 20–40% automated.

3. Domain Control Validation (DCV) Readiness

Objective: Assess whether your DCV methods survive the shift to 10-day reuse in Phase 3 (March 2029). This is harder than the 47-day headline.

☐	Current DCV methods documented for each CA relationship
☐	Identified which DCV methods you're using (DNS-01, HTTP-01, TLS-ALPN-01, email, manual file)
☐	Aware that email-based DCV is being sunset by March 2028 (SC-080/SC-090/SC-091 — only DNS-01, HTTP-01, TLS-ALPN-01 survive)
☐	DNS-01 automation assessed: do you have API access to your DNS provider(s)?
☐	DNS provider API credentials configured and tested (Cloudflare, Route53, Azure DNS, GCP Cloud DNS, etc.)
☐	Split-horizon DNS evaluated — internal vs external zones won't break automated validation
☐	HTTP-01 feasibility assessed: can web servers serve /.well-known/acme-challenge/ automatically?
☐	TLS-ALPN-01 feasibility assessed: does your infrastructure support ACME TLS-ALPN on port 443?
☐	Wildcard certificates identified — these REQUIRE DNS-01
☐	DCV can complete without human approval for all certificates
☐	DCV automation tested end-to-end (not just “enabled in config”)

■ The 10-day DCV reuse window means ~35 domain validations per cert per year in Phase 3. DNS-01 is the only method that works for wildcards — prioritize DNS-01 automation above all else. DNS changes via ticketing system = a human dependency that won't scale.

4. ACME & Issuance Pipeline

Objective: Verify your certificate issuance pipeline can handle 8x throughput without breaking.

☐	ACME client deployed and configured (Certbot, acme.sh, cert-manager, Venafi, other CLM)
☐	ACME client version is current
☐	ACME account key management documented (storage, access, rotation plan)
☐	Rate limits understood for each CA you use (Let's Encrypt, Sectigo, DigiCert, etc.)
☐	Rate limits won't throttle at 8x renewal volume (certs × 8 renewals/year vs CA rate limits)
☐	Retry logic exists for transient failures (CA outage, network timeout, DNS propagation delay)

- ☐ Multi-SAN and wildcard certificates handled by your ACME configuration
- ☐ Staging/test environments use CA staging endpoints
- ☐ Issuance pipeline tested under simulated load (not just “it works for one cert”)
- ☐ Fallback CA relationship established for primary-CA outages

■ If you use a CLM (Venafi, Keyfactor, DigiCert Trust Lifecycle, Sectigo SCM), verify its ACME connector actually works in your deployment — many have ACME support that is available but not production-tested in your environment.

5. Deployment Automation

Objective: This is where most “automated” pipelines fail: the cert renews, but never actually gets deployed.

- ☐ Deployment is automated for every platform where certificates are installed
- ☐ Web servers (Nginx, Apache, IIS, Caddy, Traefik): automated reload/restart after cert replacement
- ☐ Load balancers (F5 BIG-IP, HAProxy, AWS ALB/NLB, Azure App Gateway): automated cert push
- ☐ CDNs (Cloudflare, CloudFront, Akamai, Fastly): automated cert update or managed renewal verified
- ☐ Kubernetes: cert-manager or equivalent handles issuance AND deployment to secrets/ingress
- ☐ Cloud services (ACM, Azure Key Vault, GCP Certificate Manager): managed renewal verified working
- ☐ Multi-node deployments handled: ALL nodes get the new cert, not just one
- ☐ Service restart/reload sequence documented and tested
- ☐ Deployment verification exists: something confirms the endpoint is serving the new cert
- ☐ Rollback plan exists if a bad cert gets deployed
- ☐ No manual steps between issuance and deployment (no copy-to-server, GUI upload, or ticket)

■ Deployment is the #1 failure point in certificate automation. F5 BIG-IP is notoriously difficult here — if you have F5s, this is probably your biggest single risk. “The CDN handles it” is only true for managed certs; custom certs uploaded to CDNs do NOT auto-renew.

6. Monitoring & Alerting

Objective: Can you detect and respond to a failed renewal before the certificate expires?

- ☐ External certificate expiry monitoring in place (not relying solely on internal CLM alerts)
- ☐ Alerts fire at appropriate intervals: 30, 14, 7, 3, 1 days before expiry
- ☐ Alert thresholds adjusted for shorter validity periods
- ☐ ACME renewal failure alerts configured (detect the failure, not the consequence)
- ☐ Deployment failure alerts configured (cert issued but not deployed = ticking time bomb)
- ☐ Post-deployment verification: automated check confirms the endpoint serves the new cert
- ☐ Alert routing goes to the right team (not a shared inbox nobody reads)
- ☐ Alert fatigue assessed: teams aren't ignoring cert alerts due to false positives

- ☐ Dashboards show renewal status across the fleet (not just per-cert)
- ☐ Monitoring covers weekend/off-hours renewals

■ At 47-day validity with renewal at day ~30, you have roughly 17 days between “renewal should have happened” and “certificate expires.” The most important alert isn’t “cert expiring soon” — it’s “renewal attempted and failed.”

7. Phase 1 Specific Readiness (March 15, 2026 — now in effect)

Objective: Confirm you're ready for 200-day (199 effective) validity. This is the dress rehearsal.

- ☐ All public TLS certificates set to renew before reaching 199-day validity
- ☐ Renewal cadence adjusted to a 6-month cycle
- ☐ DCV reuse configured for the 198-day window (not the old 398-day assumption)
- ☐ SII reuse configured for the 398-day window (unchanged in Phase 1)
- ☐ CLM tool or automation updated to recognize the 199-day max (some tools still assume 398)
- ☐ No certificates with >398-day validity still assumed valid post-March 15, 2026 (grandfathered, but verify)
- ☐ At least one full renewal cycle completed successfully with the new limits
- ☐ Monitoring thresholds adjusted for 199-day certificates

■ Phase 1 is your free trial for automation. If anything breaks at 2x throughput, fix it before 4x (Phase 2) and 8x (Phase 3). Check your CA's specific enforcement date — Sectigo began enforcing 199-day max on March 12, 2026.

8. Organizational Readiness

Objective: Technology is half the problem. The other half is people and process.

- ☐ Executive sponsor identified for the 47-day readiness initiative
- ☐ Budget allocated for CLM tooling, DNS automation, and deployment automation
- ☐ Cross-team coordination plan exists (networking, DevOps, security, application teams)
- ☐ Policy deadline set: “no manual renewals after [date]” with tracking
- ☐ Runbooks documented for: normal renewal, failed renewal, emergency replacement, CA outage
- ☐ Team trained on new procedures (not just the one person who set it up)
- ☐ Vendor relationships reviewed: CA support contacts, CLM vendor escalation paths
- ☐ Exception process defined for certificates that genuinely cannot be automated — with a plan to shrink the list
- ☐ Readiness status reportable to leadership (dashboard, scorecard, or executive summary)
- ☐ Quarterly re-audit scheduled through March 2029

■ The exception list is the most important output. Every cert on it will cause an outage when 47-day validity arrives unless you have a plan. Frame the initiative to leadership as preventing the next production outage, not as “a PKI project.”

9. Readiness Scoring & Next Steps

Objective: Summarize your audit into a defensible readiness score and plan next actions.

☐	Used the PKI Priority Planner (fixmycert.com/tools/pki-priority-planner) for a personalized action plan
☐	Prioritized Section 5 (Deployment) and Section 3 (DCV) gaps first — hardest to fix, most common failure points
☐	Next re-audit scheduled for 90 days from today

Scoring guide

90–100%	Ready — automation in place, monitoring works, team prepared
70–89%	On Track — core automation exists, gaps known and being addressed
50–69%	At Risk — significant manual dependencies remain, timeline tight
Below 50%	Critical — major gaps, immediate action needed

Next steps

Track every deadline in this document automatically — the FixMyCert Compliance Hub monitors CA/Browser Forum changes and live countdowns: fixmycert.com/compliance

Interactive version of this checklist with auto-scored progress:
fixmycert.com/checklists/47-day-readiness-audit

Need the audit paperwork done? Compliance-in-a-Box — CP/CPS templates, key ceremony script, and the documents auditors actually ask for: fixmycert.com/compliance-in-a-box