

The CA redundancy readiness checklist

Your certificates shouldn't depend on any one CA. This checklist shows how ready your organization is to run a CA redundancy strategy: two CAs connected, one console, and the ability to shift issuance with a policy change instead of a fire drill.

Work through each section and tick what's already true today. Every unticked box is a single-CA dependency worth closing before certificate lifespans drop from 200 days to 100 days in March 2027, then to 47.

Know your exposure

You can't plan for a CA event until you know which certificates depend on which CA.

We have a single, complete inventory of every certificate in our estate, public and private.

☐

We know which CA issued each certificate.

☐

Discovery covers our cloud (AWS, Azure Key Vault, Google Cloud), Active Directory and network, not just the certificates we bought.

☐

We know what share of our public certificates comes from a single CA.

☐

We've identified the business-critical services that would stop if their CA became unavailable.

☐

We know who owns each certificate and who gets alerted when it's due to expire.

☐

Plan for the five CA events

Browsers can and do remove trust from CAs, and mis-issuance can happen at any CA. Check you have a plan for each event before it happens.

Distrust: If a root program distrusts our CA, we can redirect issuance to a second CA without an emergency procurement.



Mass revocation: We can replace a large batch of certificates on short notice, on the browsers' timeline rather than ours.



Downtime: If our CA has an outage or maintenance window, urgent issuance and renewals keep moving through another CA.



Shorter lifespans: Our renewal process can absorb roughly twice as many renewals in 2027, and more again at 47 days, without a CA delay turning into an outage.



Key compromise: We can bulk revoke and replace affected certificates, with a CLM and a second issuing source ready.



Connect a second CA

Implementing CA redundancy doesn't need a migration project. Keep the CAs you already use and add a second issuing source alongside them.

We have a second publicly trusted CA connected and ready to issue, not just a contract on file.



Our backup CA is managed with the same tooling as our primary, not left as a manual or community-supported fallback.



Our private PKI (for example Microsoft CA, AWS Private CA or Google Cloud CA Service) is visible alongside our public certificates.



We can use the right CA for each job: public TLS/SSL, S/MIME and code signing, plus private certificates for internal users and devices.



Adding or changing a CA doesn't force a rip-and-replace or a re-trust of every device.



We're already issuing some certificates from the second CA, starting with new or expiring ones, so it's proven before we need it.



Run every CA from one console

Two CAs only add resilience if they share the same controls. Otherwise you've doubled the work, not the safety.

We discover, issue, renew and revoke certificates from every CA in one console.



The same certificate policies apply no matter which CA issued the certificate.



We have one audit trail and one set of reports across all CAs.



Renewals are automated (for example via ACME) across both CAs, not just the primary.



We can move issuance volume between CAs with a policy change, not a project.



Our certificate tooling connects to the rest of our stack, such as secrets management, SIEM and firewalls.



Prove the switch works

A fallback you've never used is a plan on paper. Rehearse it while nothing is broken.

We've documented who decides to shift issuance to the second CA, and when.



We've tested moving a set of renewals from one CA to the other.



We've run a bulk revoke-and-replace drill and know how long it takes.



Our incident response plan names a CA distrust or outage as a specific scenario.



We review our CA mix at least once a year, and again when lifespans change.



How did you score?

We've documented who decides to shift issuance to the second CA, and when.



23-28

CA redundancy ready

A CA event becomes a policy change, not an outage.



12-22

Partly covered

You have pieces in place, but gaps that would turn a CA event into manual work.



0-11

Single-CA dependent

Your certificate operations are tied to one vendor's roots, uptime and roadmap.



Find out where a single CA leaves you exposed

Book a 30-minute single-CA risk assessment with Sectigo. We'll map your certificate estate, flag single-CA dependencies and show how a CA-redundant setup would work with the CAs you already use.

[Book my risk assessment](#)

