

The 47-Day Toolkit: How to Use

Sectigo's 5 steps to 47-day readiness are ready for you to download. Wondering how to use each step? Check out our guide below for more information and how to use each asset.

Step 1 Awareness and discovery

Gain complete visibility of your certificate inventory.

Certificate management health check

This survey will give you a starting point to determine what certificates you have, how you manage them, and where you may have risks. [Complete this form](#) first to determine risks or gaps in your cert management and get simple next steps.

- **SCM cloud discovery guide**

Our [Cloud Discovery Guide](#) is a step-by-step instruction manual showing you how to use Sectigo Certificate Manager to discover all certificates.

- **SCM how to discover certificates video**

[This video](#) accompanies our Cloud Discovery Guide to lead you through certificate discovery in SCM and give further context to discovery.

- **Organization email template**

This [email template](#) provides you with all of the key information you need to share with your internal teams. It includes important dates, the reason for the change, implications for your business, and what's at risk if the team does not prepare. This functions as an internal awareness campaign for a smoother path to 47-day readiness and automation down the line.

Step 2 Vendor technology inventory

Map vendors and systems to avoid disruptions and streamline renewals.

The 47-day workshop steps 2 & 3

This [workbook](#) helps your team build a clear project plan and accelerate your path to automation. The goal of Step 2 is to establish clear links between certificates and the technology vendors that rely on them to reduce unexpected outages, prioritize critical systems, and ensure clear ownership and accountability across your infrastructure.

Step 3 Automation mapping

Build a prioritized roadmap for automation and PQC readiness.

The 47-Day workshop steps 2 & 3

This is the [same spreadsheet](#) from Step 2. The goal of Step 3 is to build and prioritize a clear plan to shift from manual to automated certificate renewals, while also assessing PQC readiness as part of the process.

- **ACME first cheat sheet**

Use this [cheat sheet](#) as a reference point when mapping your environment and identifying where ACME fits, and where to extend beyond it. We've included examples of ACME-compatible systems and clients that integrate well with SCM.

- **DCV automation checklist**

Domain Control Validation (DCV) is a key part of the move to 47-day certificates. To effectively manage DCV changes, we've created this [checklist](#) to evaluate your organization's readiness.

- **Sectigo automation datasheet**

Sectigo's [Automation Datasheet](#) highlights SSL/TLS-compatible automation options, whether connected through ACME or built natively. It provides key insights, feature details, and integration options to help you choose the right automation approach for your environment.

Step 4 Rollout plan

Align teams with a clear plan, roles, and accountability.

47-day readiness project plan

This [GANTT chart](#) gives you a project plan to personalize to your business, schedule, and track your progress along your journey to automation and 47-day lifespans. It features Sectigo's 5 Steps to 47-Day Readiness, guidelines, and a calendar to ensure timeliness.

- **47-day readiness RACI**

It's critical to ensure your teams are aligned on the goals and responsibilities in preparing for 47-day certificates. Use this [RACI template](#) to identify your key stakeholders and to drive team alignment.

- **Internal communication toolkit**

This [toolkit](#) gives you copy and guidance on how to educate, align, and instruct your team members. It includes an executive summary to brief the team on 47-days, a recommendation, and project management email templates to aid your project start-up.





Step 5 Crypto agility

Build a crypto-agile, quantum-ready infrastructure that powers zero-trust, adapts to change, and keeps you compliant.

CCoE charter template

Our experts are adamant about establishing a Crypto Center of Excellence (CCoE) where all cryptographic policies exist for reference in a post-quantum world. The CCoE will enable teams to build cryptographic resilience, ensure governance compliance, and reduce operational risks. This [charter template](#) is a starting point for your organizations own charter as you solve for 47-day lifespans and become crypto-agile.

- **Cryptographic policy review checklist**

This [checklist](#) is a simple guide to ensure your team has everything you need to become crypto-agile. Use this internally and bring it to executive briefings to ensure your organization is aligned on your post-quantum policies, paths to crypto agility, and readiness.

- **CLM maturity assessment**

Don't mistake manual steps for CLM automation. A [maturity assessment](#) will identify critical gaps. Without genuine automation, your organization lacks the crypto agility required to secure and quickly adapt your PKI.



Need help?

If you have any questions on our 47-Day Readiness Toolkit, please reach out to sales@sectigo.com.

