

Executive Summary

Preparing for 47-Day TLS Certificate Lifespans

Use this template to brief your executive team on upcoming changes.

As part of an industry-wide shift in digital security standards, TLS certificate lifespans will be reduced from the current 398 days to 200 days in March of 2026 and just 47 days by 2029. This change will significantly impact how we manage digital certificates across our systems and underscores the urgent need for automation.

Why it Matters

Shorter certificate lifespans reduce the risk posed by a compromised certificate. By minimizing exposure time, we reduce risks associated with compromised certificates and ensure more frequent validation of certificate integrity and security practices.

What's Changing

The current 398-day certificate term will shrink to 47 days, requiring monthly renewals instead of yearly renewals. Manual processes will not scale, increasing the risk of outages, breaches, and compliance failures.



The Risk of Inaction

Public digital certificates play a crucial role in keeping our website secure and accessible for customers. They verify a website's identity and encrypt communications, protecting users' data. Expired certificates can lead to service disruptions and browser warnings, potentially driving customers away from our platforms, resulting in lost revenue.



We Need to Automate

Automation is essential. Adopting a Certificate as a Service (CaaS) model reduces the new operational burden on our IT staff and streamlines renewals, reduces human error, and ensures continuous compliance.

Action Plan

1. **Raise Awareness** – Educate teams and stakeholders on the impact.
2. **Discover Certificates** – Inventory all public certificates across systems.
3. **Map Automation** – Align automation tools (e.g., ACME clients) with our tech stack.
4. **Develop a Rollout Plan** – Define objectives, timelines, and responsibilities.
5. **Establish Crypto Agility** – Form a Cryptographic Center of Excellence to future-proof security.

Recommendation

Automation is essential. Adopting a Certificate as a Service (CaaS) model reduces the new operational burden on our IT staff and streamlines renewals, reduces human error, and ensures continuous compliance.

Project Management Template for the Core Team

Use our included 47-day project plan to track your progress towards readiness milestones. This email template helps your team stay on track with a weekly update. The 47-day RACI Matrix will help you identify the appropriate audience.

Subject: [Project Name] – Weekly Status Update – [Date]

Hi Team,

Here's the latest update on [Project Name] as of [Date]. Thanks to everyone for your continued collaboration and contributions!

Project Snapshot

Current Phase: [e.g., 47-Day planning step/milestone]

Overall Status: [On Track / At Risk / Delayed]

Project Lead: [Name]

Target Completion Date: [Date]

Highlights This Week

- [Brief update on a completed task or milestone]
- [Cross-team collaboration highlights or decisions made]
- [Progress metric or success indicator, if applicable]

What's Coming Up

Milestone	Owner	Due Date
[Milestone Name]	[Team/Person]	[Date]
[Milestone Name]	[Team/Person]	[Date]

Risks & Blockers

Issue	Impact	Owner	Mitigation
[Risk/Issue]	[High/Medium/Low]	[Name/Team]	[Plan or Ask]

Action Items

Task	Owner	Due Date	Status
[Action Item]	[Name/Team]	[Date]	[Not Started/In Progress/Complete]

Please feel free to reply with questions, updates, or anything that needs to be flagged. Let's keep the momentum going!

Best,

[Your Name]

[Your Role]

[Contact Info]



Change Management Email Template

Use this template to help prepare your stakeholders for reduced certificate lifespans.

Subject: Upcoming Change: TLS Certificate Lifespan Reduction – What You Need to Know

Hi Team,

As part of an industry-wide shift in digital security standards, TLS certificate lifespans will be reduced from the current 398 days to 200 days in March of 2026 and just 47 days by 2029. This change will significantly impact how we manage digital certificates across our systems.

What's Changing

- Certificates will need to be renewed more frequently. Every 200 days by March of 2026 and every 47 days by 2029.
- Manual certificate management will no longer be sustainable.
- As an organization, we will be focusing on certificate discovery, automation, and governance to avoid outages, compliance issues, and security risks.

What This Means for You

- Teams responsible for infrastructure, security, and application delivery will need to adapt to more frequent certificate renewals.
- We'll be implementing automated certificate lifecycle management (CLM) to ensure continuity and reduce operational burden.
- Training, tools, and support will be provided to help you transition smoothly.

What's Next

- We'll begin with awareness sessions and discovery workshops to identify impacted systems and stakeholders.
- A rollout plan will follow, including automation mapping and implementation timelines.
- You'll receive regular updates and resources to stay informed and prepared.

We appreciate your attention and collaboration as we make this important transition. If you have questions or would like to get involved in the planning process, please reach out to [Project Lead/IT Contact].

Best regards,

[Your Name]

[Your Title]

[Your Contact Info]

