



ETSI/IQC Quantum Safe Cryptography
Conference 2026

Tackling PQC and 47-Day Certificates in Parallel

Presented by:



June 16, 2026

© ETSI 2026. All rights reserved.

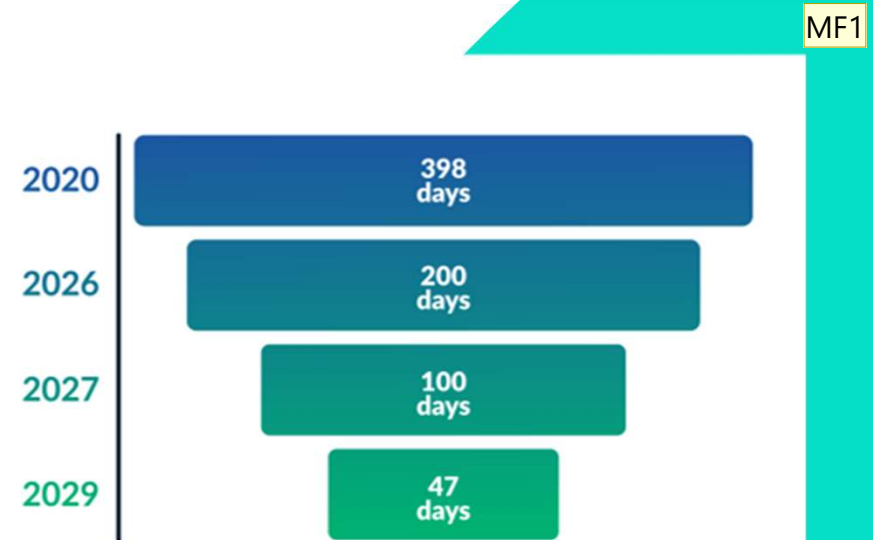
A recap: The timeline of certificate lifespans

On March, 3, 2023, **Google's** "Moving Forward, Together" roadmap laid out its intention to reduce TLS certificate validity from 398 to 90days.

In January 2025, **Apple** proposed the 47-day ballot, sponsored by Sectigo, to the CA/Browser Forum.

On April 11, 2025, this ballot was passed by the CA/Browser Forum.

As of **March 15, 2026** public TLS now has maximum term of 199 days.



Slide 2

MF1

Need to upgrade graphic.

Morgan Friedel, 2026-04-16T18:17:21.372

March 2026: The first step down & beyond

Effective date	Certificate term	Renewal cadence
March 15, 2026	199 days	Six months
March 15, 2027	99 days	Three months
March 15, 2029	46 days	Monthly



47-day TLS means 12x more work



The long-term vision:

Why do we need shorter lifespans?



The short answer...

They are safer.

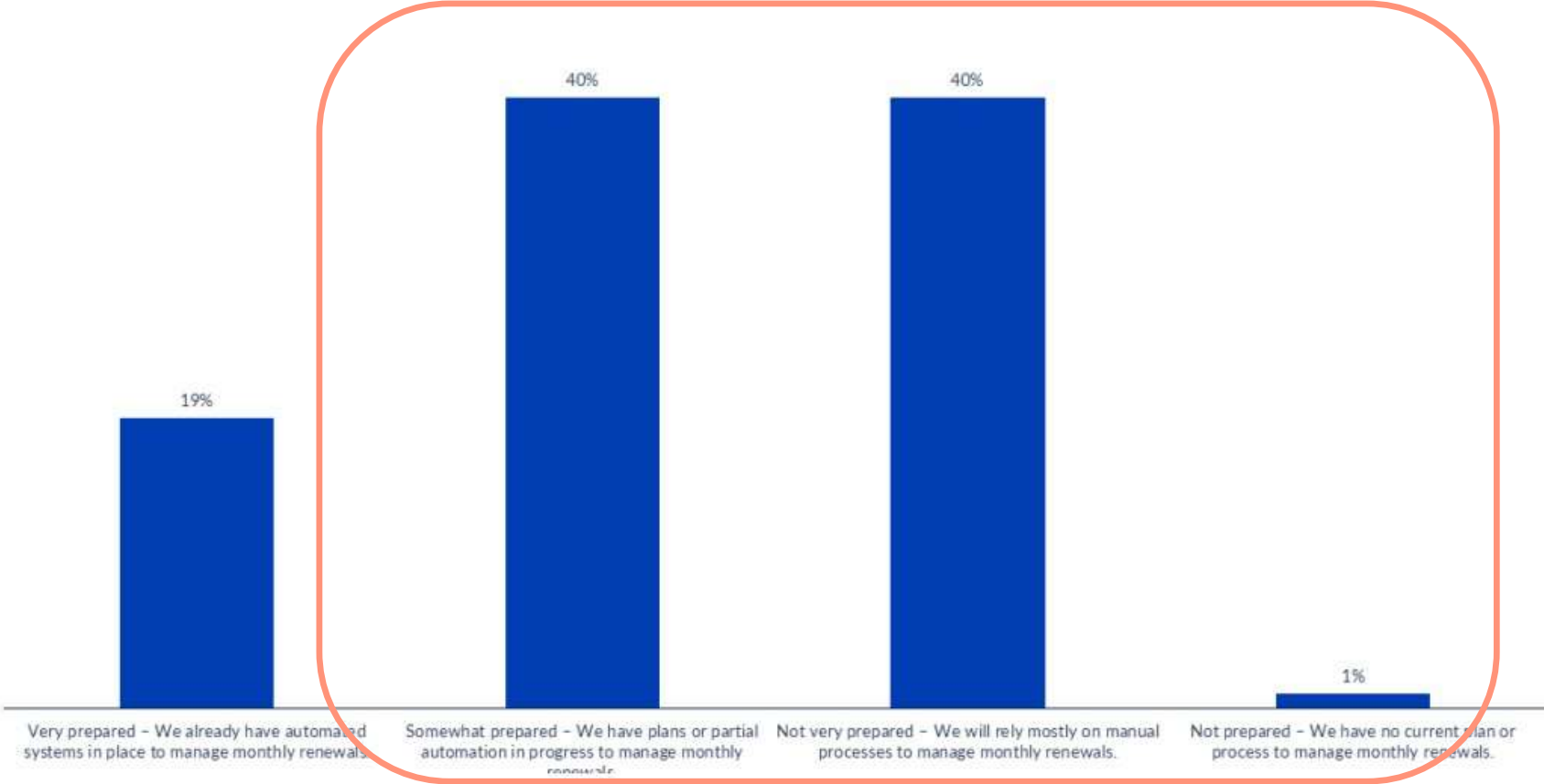
Why shorter TLS certificate lifecycles are a better choice

- Enhanced security
- Limiting outdated cryptographic standards
- Operational efficiency
- Agility and flexibility
- Adoption of best practices



Our study with Omdia shows...
Many are not ready for this change.

How prepared is your organization to transition to monthly renewals of public TLS certificates?



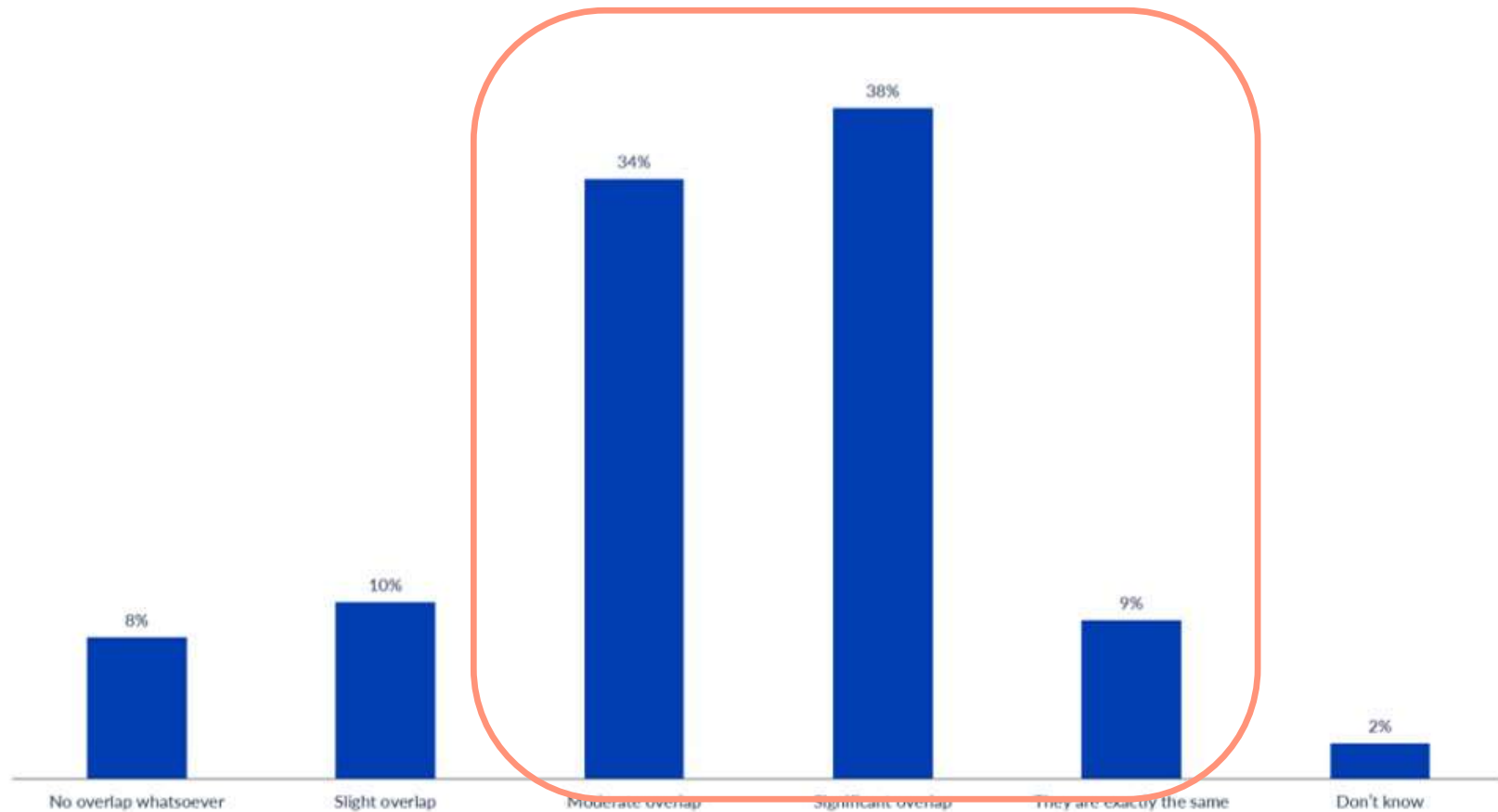
Slide 8

MF1

update graph colors

Morgan Friedel, 2026-04-16T18:25:37.996

Do you see overlaps in your organization's preparedness for 47-day TLS and post-quantum cryptography?



Quantum resilience through shorter certificate lifespans

Duplication across stakeholders

CISO

- CBOM
- Certificate upgrade path
- Cryptographic policies
- Crypto-agility

CIO

- Management and renewal
- Certificate automation
- Certificate policies
- Crypto-agility



Why prioritizing crypto-agility is essential

Static encryption can't keep up

Hardcoded algorithms and long-lived certificates limit your ability to respond to emerging threats like quantum computing.

Compliance and regulatory pressure is increasing

Government and industry bodies are mandating crypto-agility and shorter certificate lifespans.

Definition



Crypto-agility:

The ability to quickly switch between cryptographic algorithms and protocols without disrupting systems or services.

You don't need to be perfect, you just need to be on the right path

- The 200-day deadline is about risk reduction, not perfection
- Start by automating high-impact systems first and focus where outages would hurt most
- Gradual rollout works: pilot automation, refine processes, then scale
- Manual processes are still valid as a stopgap, but automation must be in the plan





GOAL: Reduce human error, increase predictability, and build confidence ahead of March 2026



Prioritizing systems for automation

All automation may not be ready at the same time. Prioritize your projects.

		How critical?	
		Low	High
How difficult?	Easy	Middle	First 
	Hard	Last 	Middle



Making the case for automation...

Benefit	Manual CLM	Automated CLM	ROI Impact
Time Spent per Certificate	30–60 min	<5 min	~90% time savings
Outage Risk	High (expired certs, config errors)	Very Low	Avoids revenue loss
Staff Productivity	Low (manual tracking, troubleshooting)	High (focus on strategic work)	IT efficiency boost
Compliance Readiness	Ad hoc, spreadsheet-driven	Continuous, automated audits	Reduces audit prep time
Security Posture	Reactive	Proactive	Fewer vulnerabilities



If you liked this conversation...



ROOT CAUSES

A PKI & Security Podcast

Available on these streaming services



Slide 16

MF1 Need to update to new branding
Morgan Friedel, 2026-04-16T19:43:34.539

