

Cryptographic Policy Review Checklist

As the industry accelerates toward 47-day certificate lifespans, traditional cryptographic policies, often built for long-lived certificates and manual processes, are no longer sufficient. Organizations must now adopt agile, automated, and scalable approaches to certificate management to avoid outages, meet compliance requirements, and keep pace with security best practices. This checklist helps you evaluate whether your current policies are ready for this shift and identifies critical gaps that could hinder your ability to operate securely in a short-lived certificate environment.

Governance and ownership

Question	Yes	No	Action Required
Is there a formally documented cryptographic policy?	<input type="checkbox"/>	<input type="checkbox"/>	
Is policy ownership clearly assigned to a team or role (e.g., PKI/crypto lead)?	<input type="checkbox"/>	<input type="checkbox"/>	
Is the policy reviewed and updated at least annually (or more frequently)?	<input type="checkbox"/>	<input type="checkbox"/>	
Are exception-handling processes formally documented and enforced?	<input type="checkbox"/>	<input type="checkbox"/>	

Automation and operational agility

Question	Yes	No	Action Required
Does the policy require or support automation for certificate issuance and renewal?	<input type="checkbox"/>	<input type="checkbox"/>	
Are short-lived certificates (≤ 47 days) explicitly addressed and operationally supported?	<input type="checkbox"/>	<input type="checkbox"/>	
Are DevOps and CI/CD environments addressed with automation guidance?	<input type="checkbox"/>	<input type="checkbox"/>	
Can expired certificates be automatically detected and remediated?	<input type="checkbox"/>	<input type="checkbox"/>	

Documentation and scope

Question	Yes	No	Action Required
Are key processes (issuance, renewal, revocation) clearly documented?	<input type="checkbox"/>	<input type="checkbox"/>	
Is inventory completeness a stated requirement?	<input type="checkbox"/>	<input type="checkbox"/>	
Are internal CA and third-party CA usage policies defined?	<input type="checkbox"/>	<input type="checkbox"/>	
Are non-production environments (dev, test) covered by policy?	<input type="checkbox"/>	<input type="checkbox"/>	

Scalability and compliance

Question	Yes	No	Action Required
Does the policy support high-frequency certificate rotations (e.g., every 47 days)?	<input type="checkbox"/>	<input type="checkbox"/>	
Are monitoring and alerting requirements included?	<input type="checkbox"/>	<input type="checkbox"/>	
Are auditability and reporting requirements clearly defined?	<input type="checkbox"/>	<input type="checkbox"/>	
Can the policy scale to cloud-native, containerized, and edge environments?	<input type="checkbox"/>	<input type="checkbox"/>	

Final review



10–13 “Yes” answers

Your policies are likely ready or near-ready for 47-day agility.



6–9 “Yes” answers

Action required to prioritize automation and documentation gaps.



<6 “Yes” answers

Policies need overhaul to support secure short-lived certificate operations.