Government Cryptographic Governance Checklist

ENTRUST

Are You Prepared for the Next Generation of Cryptographic Security?

Government agencies must protect sensitive data, sustain essential services, and meet oversight requirements. Yet aging infrastructure, distributed and cloud environments, third-party dependencies, and limited resources can complicate consistent cryptographic governance. As quantum, machine identity, and AI risks grow, this checklist helps public-sector organizations assess cryptographic security maturity.

HOW TO USE THIS ASSESSMENT

Select one response for each question. To enable automatic point tallying, download this PDF and open it in the Adobe Acrobat app.

Yes (Implemented and documented) = 2 points
Partially (Incomplete or inconsistently implemented) = 1 point
No – Absent or unknown = 0 points

DATA PROTECTION & KEY CONTROL	YES	PARTLY	NO
Have you identified the most critical and sensitive data assets within your organization?			
Can you demonstrate who owns and controls the cryptographic keys protecting those assets?			
Are encryption keys protected separately from the data they secure?			
Can key management policies be enforced consistently across cloud, hybrid, and on-premises environments?			
Do you have centralized visibility into cryptographic controls across departments, agencies, and business units?			

OPERATIONAL RESILIENCE & RECOVERY	YES	PARTLY	NO
Can critical services recover following a ransomware incident?			
Can you maintain access to critical keys if a cloud service, technology provider, or infrastructure platform becomes unavailable?			
Have cryptographic recovery procedures been tested through disaster recovery exercises?			
Can critical workloads continue operating during major service disruptions?			
Do backup and recovery environments follow the same governance standards as production systems?			

CLOUD, SOVEREIGNTY, & THIRD-PARTY RISK	YES	PARTLY	NO
Do you know which cloud services currently manage cryptographic keys on your behalf?			
Can your organization maintain independent control of encryption keys for critical workloads?			
Have you assessed cryptographic risks associated with third-party platforms and service providers?			
Can you support enhanced assurance models such as customer-controlled key management when required?			
Can you demonstrate cryptographic governance to auditors, oversight bodies, or security assessors?			

CRYPTOGRAPHIC VISIBILITY & MODERNIZATION	YES	PARTLY	NO
Do you maintain a current inventory of keys, certificates, secrets, HSMs, and machine identities?			
Can you identify unmanaged certificates, vulnerable keys, and unknown dependencies?			
Can you generate a cryptographic inventory for critical applications and services?			
Do security teams have visibility into cryptographic risk across the organization?			

POST-QUANTUM READINESS	YES	PARTLY	NO
Have you identified systems that may be vulnerable to future quantum computing threats?			
Do you understand which keys, certificates, and applications may require migration?			
Do you have a strategy for post-quantum cryptographic modernization?			
Can your PKI support future cryptographic algorithm transitions?			
Is post-quantum planning incorporated into broader cybersecurity and modernization initiatives?			

AUTOMATION & SCALE	YES	PARTLY	NO
Are cryptographic controls deployed and maintained through automation wherever practical?			
Can key management and certificate management processes be standardized across environments?			
Can cryptographic policies be enforced consistently through infrastructure automation?			
Do platform and operations teams have repeatable methods for implementing cryptographic controls?			
Can governance and compliance requirements be applied consistently without manual intervention?			

MACHINE IDENTITY & AI SECURITY	YES	PARTLY	NO
Do you maintain visibility into machine identities across APIs, applications, cloud services, automation platforms, and AI-enabled systems?			
Are non-human identities governed according to organizational security policies?			
Can you identify which applications, services, and AI agents have access to sensitive data?			
Are machine credentials, secrets, API tokens, and service accounts centrally managed?			
Do you have a strategy for establishing trusted identities for AI-enabled systems and autonomous workloads?			
Subtotals	0	0	
TOTAL	0		

Your Results

Add your scores to calculate a total out of 70. These ranges are directional indicators of maturity, not compliance determination.

0-24 EMERGING

Immediate opportunities exist to improve cryptographic governance, resilience, and visibility.

25-48 DEVELOPING

Foundational controls are in place, but modernization and governance gaps remain.

49-70 ADVANCED

Strong cryptographic governance, operational resilience, and readiness for machine identity and post-quantum requirements.

Ready to take the next step? Explore the interactive demo to see how greater cryptographic visibility can help you discover and manage cryptographic assets, identify ownership and risk, and build a stronger foundation for resilience and post-quantum readiness.

Need expert guidance? Talk with an Entrust specialist about strengthening your cryptographic visibility, resilience, and post-quantum readiness.

ENTRUST
SECURING A WORLD IN MOTION