Financial Services Cryptographic Resilience Checklist

Are you prepared for the next generation of cryptographic governance, resilience, and machine identity security?

Financial Institutions face growing pressure to strengthen resilience, protect sensitive data, manage third-party risk, and prepare for quantum and AI-driven threats. You cannot protect keys, certificates, secrets, and machine identities without knowing where they are, what they protect, and who owns them. This checklist helps identify gaps in cryptographic visibility, governance, resilience, and future readiness, and guides practical improvements.

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

CRYPTOGRAPHIC VISIBILITY	YES	PARTLY	NO
Can you maintain a current inventory of cryptographic assets, including keys, certificates, secrets, HSMs, and machine identities?			
Do you know where cryptographic assets are deployed across cloud, SaaS, on-premises, backup, storage, and hybrid environments?			
Can you identify who owns and is accountable for each critical cryptographic asset?			
Can you generate a cryptographic inventory for critical applications, business services, and technology platforms?			
Can you quickly identify expired certificates, unmanaged keys, shadow secrets, or orphaned cryptographic assets?			

OWNERSHIP, CONTROL, & CUSTODY	YES	PARTLY	NO
Can you demonstrate ownership, possession, and control of encryption keys that protect sensitive business and customer data?			
Are encryption keys managed independently from the data they protect?			
Can you retain control of critical cryptographic assets during a cloud provider, SaaS provider, or ICT service disruption?			
Can you support customer-controlled key models when required?			
Can you provide evidence of cryptographic custody during audits, due diligence activities, or regulatory reviews?			

OPERATIONAL RESILIENCE	YES	PARTLY	NO
Have you identified the critical business services that depend on cryptographic controls?			
Can critical services continue operating if a key management platform becomes unavailable?			
Have cryptographic recovery procedures been documented and tested?			
Can you demonstrate resilience during cyber incidents, ransomware attacks, cloud outages, or supplier disruptions?			
Are cryptographic controls incorporated into operational resilience and third-party risk management programs?			

CRYPTOGRAPHIC RISK MANAGEMENT	YES	PARTLY	NO
Can you identify which cryptographic assets present the highest organizational risk?			
Do security teams have visibility into cryptographic risks across business units and technology silos?			
Can risk, audit, compliance, and security teams work from a common view of cryptographic risk?			
Can governance gaps be prioritized according to business impact?			
Does leadership have access to meaningful metrics that track cryptographic risk and security posture?			
POST-QUANTUM READINESS	**YES**	**PARTLY**	**NO**
Have you identified cryptographic assets that could be affected by future quantum computing threats?			
Do you maintain an inventory that can support post-quantum migration planning?			
Do you have a documented roadmap for post-quantum readiness?			
Can you assess the impact of cryptographic algorithm changes across critical systems?			
Can your PKI and certificate infrastructure support modern and hybrid cryptographic approaches during migration?			
MACHINE IDENTITY & AI SECURITY	**YES**	**PARTLY**	**NO**
Do you maintain visibility into machine identities across applications, workloads, APIs, containers, and cloud services?			
Are machine identities governed to the same standard as human identities? Can you identify which machine identities have access to sensitive systems and cryptographic material?			
Can you identify which machine identities have access to sensitive systems and cryptographic material?			
Are secrets and credentials used by automated systems centrally managed and protected?			
Do you have a strategy for securing AI agents and autonomous workloads with trusted identities?			
Subtotals	0	0	
TOTAL	0		

Your Results

Add your scores to calculate a total out of 60. These ranges are directional indicators of maturity, not compliance determination.

0-20 EMERGING

Significant gaps may exist in cryptographic visibility, governance, resilience, or machine identity security.

21-40 DEVELOPING

Foundational controls are in place, but opportunities remain to strengthen governance, resilience, and future readiness.

41-60 ADVANCED

Strong maturity across cryptographic governance, operational resilience, and emerging security 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