

Protecting Financial Institutions in a Regulated World

Cybersecurity, compliance, and resilience services for banks, lenders, payments, fintech, insurance, and regulated service providers. One partner for governance, assurance, testing, response, and managed defense.

Financial institutions and the companies that support them face more pressure than ever to prove security maturity. Customers want defensible assurance. Regulators expect stronger oversight. Boards want clear accountability.

Serket-Tech Security helps financial organizations build trust faster, reduce audit friction, strengthen third-party oversight, and improve cyber resilience through coordinated governance, validation, and ongoing operational support.



Strengthen Vendor and Supply Chain Oversight

Improve service provider reviews and third-party assurance by strengthening control mapping, validation, and reporting.



Build Trust Faster

Support exams, board reporting, and customer diligence with controls that are designed, operating, and backed by evidence.



Reduce Audit and Procurement Friction

Turn questionnaires, audits, and framework requests into a clearer assurance story built on recognized standards and disciplined execution.



Improve Resilience Across the Business

Link governance, testing, monitoring, and incident preparation to better prepare teams for fraud, ransomware, outages, and scrutiny.



A Broad Security and Compliance Portfolio

Financial organizations need more than a single audit path. They need coordinated services that support examiner expectations, protect customer data, reduce operational risk, and strengthen third-party assurance.



Executive Advisory and Future Risk

vCISO support, board reporting, AI governance, cryptographic risk review, and post-quantum planning.



Managed Security Services

Threat monitoring, endpoint protection, MDR support, alert triage, and continuous control monitoring.



Regulatory Alignment and GRC

GLBA Safeguards, FFIEC-aligned governance, risk assessments, policy programs, control mapping, and board-level reporting.



Incident Response and Resilience

Response planning, tabletop exercises, breach support, forensics coordination, business continuity alignment, and recovery guidance.



Third-Party and Vendor Risk

Vendor due diligence, inherited-control review, concentration-risk support, and stronger oversight workflows.



Penetration Testing

Internal and external network testing, web application testing, cloud testing, and prioritized findings.



Assurance and Framework Programs

SOC 2 readiness, HITRUST path support, PCI DSS preparation, evidence planning, remediation guidance, and audit coordination.



Security Assessments and Testing

Security posture reviews, architecture analysis, vulnerability assessments, cloud reviews, and remediation planning.



How Buyers Can Engage Serket-Tech Security

Clients can start with a focused program and expand as needs mature.

1. Regulatory Readiness and Assurance

Built for banks, lenders, fintech, payments, and service providers that need a stronger trust story for customers, partners, regulators, and examiners.

What It Can Include

- GRC and policy program design
- GLBA, NYDFS, FFIEC, and customer control mapping
- SOC 2 readiness and audit support
- HITRUST path support when clients need stronger third-party assurance
- Evidence planning, remediation, and examiner response support

2. Security Validation and Hardening

Built for teams that need to find gaps, test defenses, and reduce exposure before an audit, product launch, examiner review, or major diligence cycle.

What It Can Include

- Security posture and architecture reviews
- Vulnerability assessments and prioritized remediation planning
- Internal, external, cloud, and web penetration testing
- Control validation tied to fraud, payments, and availability risk
- Tabletop exercises for leadership and response teams

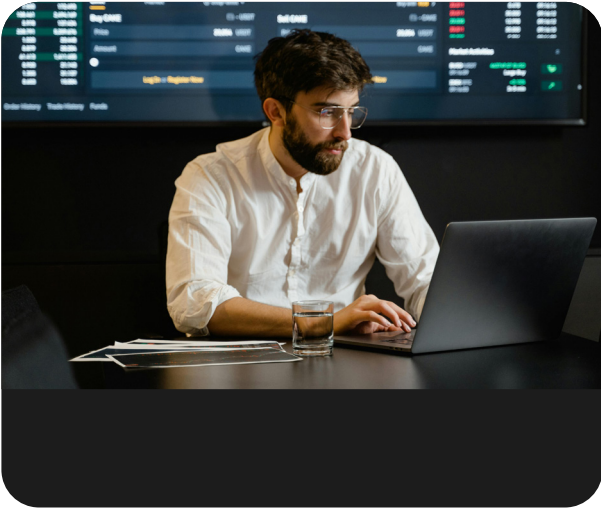
3. Continuous Operations and Resilience

Built for organizations that want security readiness to become an operating model rather than a one-time project.

What It Can Include

- Managed detection and response support
- Control monitoring, evidence collection, and issue tracking
- Third-party risk workflows and recurring assurance support
- Incident response retainers and crisis preparation
- Executive reporting and ongoing program steering





Why Serket-Tech Security

Serket-Tech Security provides financial organizations with a single partner for hands-on security execution, validation, and ongoing operational support. We help clients build a defensible program across readiness, remediation, testing, and operations.

Who We Serve

- Banks, credit unions, lenders, and non-bank financial institutions
- Fintech, payments, and embedded finance platforms
- Insurance, wealth, and capital markets firms
- SaaS and service providers selling into regulated financial markets

Oversight and Standards

- One partner across strategy, remediation, testing, and operations
- Delivery aligned to financial-sector control expectations and scrutiny
- Coverage for assurance, response, vendor risk, and managed defense
- A model that can start as a project and continue as an operating program

01



Assess

Scope business lines, systems, and control expectations.

02



Prioritize

Rank gaps, regulator pressure, and business risk.

03



Implement

Build policies, controls, evidence, and workflows.

04



Validate

Test, remediate, and prepare for audit or review.

05



Operate

Monitor, control health, and sustain readiness year-round.

Build a Program that is Customer-Ready, Audit-Ready, and Board-Ready

Engage Serket-Tech Security for a readiness workshop, service portfolio review, or managed program design.