nexustek

THE FINANCIAL SERVICES IT PLAYBOOK

How mid-market banks, insurers, and financial firms stay audit-ready, cyber-resilient, and competitive — without building an enterprise IT organization.

BANKING · INSURANCE · ASSET MANAGEMENT · CAPITAL MARKETS · PAYMENTS

SECTION 01

The Landscape

Five pressures. One IT team.
The math doesn't work.

Five Core Pressures on Mid-Market Financial Institutions

Regulatory expansion, escalating threats, AI competition, aging infrastructure, and talent shortage — all at once. Mid-market financial institutions are attempting to manage five simultaneous pressures with IT teams resourced for two.

$6.08M

Average financial services breach cost — highest of any industry

IBM COST OF A DATA BREACH, 2024

Nov 2025

NYDFS Phase 3 active — enhanced MFA and asset inventories now enforceable

NYDFS / CENTRALEYES.COM, 2025

20×

Increase in deepfake attacks over 3 years at financial institutions

FEDERAL RESERVE VICE CHAIR BARR, APR 2025

76%

Of financial services firms increasing AI investment in 2024–25

EY FINANCIAL SERVICES AI SURVEY, 2024

KEY DATA POINT

Building a 24/7 SOC internally costs $400,000+ in salaries alone — four analysts plus a SOC manager before tools, training, or turnover. (Glassdoor / Salary.com benchmarks, 2024)

KEY DATA POINT

IT downtime costs an average of $5,600 per minute — amplified during market hours, claims surges, and peak transaction periods. (NRI Network Solutions, 2025)

> Mid-market financial institutions are attempting to manage five simultaneous pressures with IT teams resourced for two. The institutions navigating this moment have recognized that internal headcount alone cannot solve all five at once.

— NexusTek Financial Services Practice

Five Core Challenges

These challenges compound. Regulatory requirements create documentation burdens that stretch internal teams. Talent constraints leave security monitoring gaps. Legacy infrastructure expands the attack surface.

01

Regulatory compliance is reactive, not proactive

NYDFS Phase 3, OCC third-party risk, FINRA, AI governance — each update creates documentation obligations internal teams address at exam time, not continuously.

VCIO ADVISORY

02

Cybersecurity can't keep pace with threat sophistication

AI-enabled phishing, deepfake fraud, and ransomware with data exfiltration — mid-market institutions face the same threat landscape as large banks with smaller teams.

24/7 SOC

03

Public cloud creates compliance gaps regulated firms can't afford

Core banking, policy admin, and portfolio management are stable workloads. One-size-fits-all public cloud can't deliver the granular control and audit-ready SOC reporting examiners expect.

PRIVATE CLOUD

04

AI adoption stalls without compliant infrastructure

Fintechs are deploying fraud detection and credit assessment at scale. Traditional institutions are paralyzed — afraid of model risk, shadow AI liability, and regulatory exposure.

AI IMPLEMENTATION

05

Talent constraints prevent scaling IT and security

Security engineers, compliance analysts, and SOC analysts choose larger banks and fintechs. Mid-market institutions can't compete at those salary levels.

CO-MANAGED IT

Regulatory Context

NYDFS, OCC, FINRA, SEC, PCI DSS, and GLBA have moved from guidance to enforced standards with documented penalties. Each creates specific IT control requirements — MFA, SOC reporting, incident response, third-party risk documentation.

NEXUSTEK'S ROLE

Implement and manage the IT controls these frameworks require — and produce the audit-ready documentation examiners expect. NexusTek does not certify compliance or provide legal counsel.

NYDFS Phase 3 + OCC Third-Party Risk

BANKING · INSURANCE · MORTGAGE

- Enhanced MFA for all users — enforceable since November 2025
- Formal asset management policies with documented RTOs
- SOC 1 and SOC 2 Type II reports from all IT vendors
- Unified third-party risk documentation across OCC, Fed, and FDIC

FINRA · SEC · PCI DSS 4.0

CAPITAL MARKETS · ASSET MANAGEMENT · PAYMENTS

- FINRA: tested BCP with documented RTOs/RPOs for trading systems
- SEC: 48-hour incident notification, written cybersecurity policies
- PCI DSS 4.0: enforceable since March 2024 — cardholder data segmentation, quarterly scans
- OCC AI model governance: inventory, validation, ongoing monitoring

SECTION 02

Real Clients

Proven in federally regulated financial services.

SOUTHEAST BANK

SIX YEARS. ZERO AUDIT ISSUES.

A federally regulated community bank.
State and federal examinations. Every year.
Not one finding related to NexusTek.

Client profile	Federally regulated community bank, multiple states, 24/7 operations
Regulatory environment	OCC, Federal Reserve, FDIC — annual state and federal examinations
Engagement duration	Six years and ongoing
Headline result	Zero audit issues related to NexusTek across six years of examinations

THE SITUATION

- Federally regulated community bank, multiple states, 24/7 operations
- Required SOC 1 and SOC 2 documentation examiners could verify on demand
- Public cloud evaluated and rejected — compliance gaps, variable billing
- Needed a long-term infrastructure partner, not a vendor relationship

WHAT NEXUSTEK DELIVERED

- NexusTek Private Cloud hosted in Tier 4/5 data centers
- SOC 1 Type II and SOC 2 Type II reporting, delivered annually
- Hybrid cloud integration with on-premises banking systems
- 24/7 remote hands, infrastructure management, incident response
- Monthly vCIO advisory — IT policy, compliance planning, exam support

> NexusTek understands what regulators expect, they're familiar with the audit process, and they're always ready to provide the documentation and support we need.

— Joe Littleton, CISO, SouthEast Bank

> NexusTek is a true partner to SouthEast Bank. Their engineers are an extension of my team — and they've always come through.

— SouthEast Bank Executive

6 Years
Zero audit issues across state and federal examinations

99.99%
Uptime SLA, NexusTek Private Cloud

SOC 1+2
Type II reporting delivered annually as standard

GROWING MORTGAGE LENDER

COMPLETE MODERNIZATION. ZERO ADDED HEADCOUNT.

A growing mortgage lender with limited internal IT needed to modernize infrastructure, strengthen cybersecurity, and scale for growth — without disrupting operations or hiring.

Client profile	Mortgage lender, 200+ employees, distributed branches
Challenge	Aging infrastructure, limited IT staff, rising compliance demands, growth through acquisitions
Headline result	Complete infrastructure modernization across distributed branches, zero added headcount

THE SITUATION

- Aging servers and legacy tape-based backup systems straining performance
- Limited internal IT staff managing multiple branches simultaneously
- Rising cybersecurity and compliance demands exceeding internal capacity
- Growth through new branches and acquisitions required scalable IT model

WHAT NEXUSTEK DELIVERED

- Co-managed IT with 24/7 help desk and onsite engineering support
- Complete server and laptop refresh; tape backup replaced
- Microsoft 365 deployment and ongoing management across all branches
- Azure AD, advanced email filtering, employee security training
- Monthly vCIO sessions — compliance planning, capital investment decisions

WHY THIS MATTERS

Co-managed IT doesn't replace internal teams — it extends them. The mortgage lender's internal IT maintained oversight and strategic direction throughout. NexusTek delivered execution, 24/7 coverage, and the specialized expertise they didn't have bandwidth to build. The company is now positioned to grow through new branches and acquisitions without added IT complexity.

SECTION 03

What We Do

Five service pillars. One partner.
Nothing left uncovered.

Five Service Pillars

01 **Private Cloud** INFRASTRUCTURE	Dedicated private cloud in Tier 4/5 data centers — granular control, data sovereignty, and audit-ready SOC reporting that public cloud's shared-tenant model cannot deliver. 99.99% uptime SLA with transparent fixed-cost billing. SOC 1 Type II and SOC 2 Type II reporting included as standard — satisfying OCC, Fed, FDIC, and NYDFS third-party risk documentation requirements.
02 **24/7 SOC** SECURITY OPERATIONS	Continuous threat monitoring, detection, and incident response across endpoints, cloud, and on-prem. NYDFS-compliant MFA enforcement. Threat intelligence, EDR, log analysis and correlation. Mean time to detect reduced from days to minutes — without adding internal security headcount. $400K+ in salary savings vs. building in-house.
03 **vCIO Advisory** STRATEGIC GUIDANCE	Monthly sessions translating NYDFS, FINRA, OCC, and SEC requirements into actionable IT policy and compliance frameworks — before the exam cycle, not during it. Technology roadmapping, third-party risk management, vendor evaluation. Regulatory exam support included: documentation preparation, gap assessments, and examiner response coordination.
04 **Co-Managed IT** EXECUTION + COVERAGE	Your team maintains oversight and strategic direction. NexusTek handles execution, 24/7 help desk, infrastructure management, patch management, and backup and disaster recovery. Example: Growing Mortgage Lender — complete infrastructure modernization across distributed branches, zero added head-count.
05 **AI Implementation** FINANCIAL SERVICES USE CASES	Fraud detection, transaction monitoring, credit assessment, loan processing, and KYC profiling deployed with model governance frameworks, AI system inventories, and regulatory controls built in from day one. Eliminates shadow AI risk. OCC, SEC, and FINRA-aligned documentation included — AI system inventory and model governance framework ready for your next examination.

By Segment

Banking

Community banks · Commercial banks · Credit unions

> *"How are you handling NYDFS Phase 3 MFA and asset inventories — and will your vendor's SOC reports hold up in your next exam?"*

NYDFS PHASE 3
OCC THIRD-PARTY RISK
FFIEC

Insurance

Carriers · Agencies · MGA · Insurtech

> *"How are you ensuring business continuity if your policy admin system goes down during renewal season or a claims surge?"*

NYDFS (NY CARRIERS)
STATE DEPT. EXAMS
HIPAA

Asset Management

RIAs · Hedge funds · Wealth managers

> *"What happens to client reporting if your portfolio system is unavailable during quarter-end — and do you have 24/7 DR support?"*

SEC CYBER RULES
48-HOUR NOTIFICATION
AI GOVERNANCE

Capital Markets

Broker-dealers · Trading firms · Clearing

> *"What's your RTO if your trading platform goes down at market open — and does your provider deliver 99.99% uptime during trading hours?"*

FINRA BCP
TRADE SURVEILLANCE
ALGO TRADING REGS

SECTION 04

Why NexusTek

Proven in federally regulated financial services. Not a generalist MSP.

WHY NEXUSTEK

Six Years, Zero Audit Issues

SouthEast Bank — six years across state and federal banking examinations with zero issues related to NexusTek. SOC 1/SOC 2 reporting, third-party risk documentation, and compliance frameworks that hold up under examiner scrutiny.

vCIO Advisory That Prevents Findings

Monthly sessions that translate NYDFS, FINRA, OCC, and SEC requirements into executable IT policy — before exam time, not during it. Strategic IT leadership without hiring a full-time executive.

Private Cloud Built for Regulated Firms

Tier 4/5 data centers, 99.99% uptime SLA, data sovereignty, and audit-ready SOC reporting. Transparent fixed-cost billing — no consumption surprises. Chosen by SouthEast Bank over public cloud.

AI With Governance From Day One

Deploy fraud detection, transaction monitoring, and credit assessment with OCC, SEC, and FINRA-aligned model governance built in — not bolted on after deployment. Eliminate shadow AI liability.

24/7 SOC Without the Headcount

$400K+ to build internally. NexusTek delivers continuous monitoring, threat detection, and NYDFS-compliant MFA enforcement at a fraction of the cost — without expanding your team.

Fixed-Cost Billing, No Cloud Surprises

Full visibility into IT spend every month. No usage spikes, no data egress fees, no budget overruns. Infrastructure that won't create audit findings and won't surprise your CFO.

6 Yrs	99.99%	100%	1,400+	~30 yrs
SouthEast Bank — zero audit issues	Uptime SLA, Private Cloud	Cloud migration success rate	Active clients company-wide	IT services experience

Schedule a Compliance Assessment

A 30–60 minute session that maps your current environment against your active regulatory frameworks — NYDFS, OCC, FINRA, PCI DSS. Gap analysis. Prioritized remediation roadmap. No cost. No commitment.

WHAT HAPPENS IN THE ASSESSMENT

Your current IT environment is mapped against the regulatory frameworks active for your institution. Control gaps, documentation gaps, and infrastructure gaps are identified. You receive a prioritized remediation roadmap and an honest view of where NexusTek can support — and where you may not need outside help.

or contact us to learn more at
nexustek.com/finserv

Sources: IBM Cost of a Data Breach Report (2024) · NYDFS Cybersecurity Regulation enforcement timeline (centraleyes.com, 2025) · Federal Reserve Vice Chair Michael Barr statement on deepfake attacks (April 2025) · NRI Network Solutions — The Cost-Saving Benefits of Managed Services (2025) · EY Financial Services AI Survey (2024) · Glassdoor/Salary.com SOC analyst salary benchmarks (2024) · NexusTek client data: SouthEast Bank and Growing Mortgage Lender engagements (internal)

nexustek.com · (877) 470-0401 · info@nexustek.com