PRASAD N. SHENOY

Delaware, OH • (201) 916-4851 • prasad.shenoy@gmail.com • linkedin.com/in/prasadshenoy

CISO | CYBERSECURITY EXECUTIVE

Enterprise security leader with 20+ years turning security into a business enabler. I build risk-aligned programs that improve regulatory posture, accelerate cloud/AI adoption, and reduce loss exposure—while giving boards clear, decision-ready visibility. Recently operated in startup-scale conditions, delivering outsized outcomes with a compact, high-caliber team; previously stewarded seven-figure initiatives in global, regulated environments. Strengths span board reporting, Zero Trust identity, GenAI security assurance, AppSec governance, and offensive security—driving measurable maturity gains and positive exam outcomes.

Strategic Impact Areas

Board & Regulator Confidence • Risk/Cost Reduction • Secure Velocity (cloud/AI) • Product & Data Trust • Talent Building • Third-Party Risk Control • Metrics & Accountability

EXPERIENCE

U.S. FinTech — Senior Director, Cybersecurity | Jul 2023–Present

Business impact: Built a risk-aligned security program that strengthened regulatory posture, de-risked AI adoption, and simplified identity—delivering enterprise-grade outcomes in startup-scale operating conditions.

Key Achievements

- Made risk decision-ready for executives by operationalizing NIST 800-53/CSF with tiered KRIs/KPIs and quarterly board briefings—clarifying investment trade-offs and remediation sequencing.
- Enabled controlled GenAI adoption (Amazon Bedrock, Amazon Q, agentic patterns) through architecture guardrails, data-handling standards, and monitoring—allowing innovation without breaching compliance boundaries.
- Aligned control objectives and evidence to SOC 2 Trust Services Criteria and NIST 800-53 v5/CSF, streamlining audit requests and reducing duplicate assessments.
- Contained blast radius with identity segmentation (corporate vs product vs DevOps) and lifecycle automation (Okta, SailPoint, PAM)—reducing access sprawl and review fatigue.
- Partnered with HR/Comms to scale security awareness and phishing campaigns; tuned training by role and lowered repeat-click rates through targeted follow-ups.
- De-risked third-party velocity by delivering 50+ security assessments; partnering with TPRM/Legal/Procurement to codify minimum controls and security language into contracts —preserving onboarding speed while tightening obligations and evidence.
- Improved assurance coverage by expanding red teaming, targeted pen tests, and vulnerability playbooks—shifting from reactive fixes to planned, risk-weighted sprints.
- Enhanced resilience by updating DR/BCP playbooks and running tabletop exercises (ransomware + third-party outages), clarifying escalation paths and closing gaps identified in testing.

Key Results

- Material YoY maturity uplift and no major exam findings; positive regulator/auditor feedback on evidence quality.
- First enterprise-approved GenAI rollout under new AI policy with documented controls and monitoring.
- ~40% reduction in access-review effort and faster exception closures due to segmentation/automation.
- Lower repeat-phish rates and improved awareness metrics in targeted groups.
- ~30% faster vendor onboarding while improving supply chain risk visibility and contract enforceability.

Cisco Systems — Cyber Offensive Security Leader | Aug 2022–Jul 2023

Business impact: Pressure-tested cloud platforms and product lines to cut deployment risk and accelerate safe releases.

Key Achievements

- Industrialized adversary simulation with a formal operating model, playbooks, and coverage strategy—turning one-off tests into a repeatable control function.
- Shifted left on product risk by wiring red-team findings into dev backlogs and CI/CD checks—shortening the discover→fix cycle and preventing late-stage surprises.
- Tuned blue-team efficacy through purple-team loops with SOC/IR—raising true-positive rates and reducing alert noise.

Key Results

- Reduced pre-launch criticals by ~60% on targeted product lines.
- 3× increase in red-team coverage with near-flat operating cost.
- ~40% faster remediation for high-impact findings.

JPMorgan Chase & Co. — Executive Director & Vice President (Progressive Roles) | Jul 2013–Aug 2022

Business impact: Built and scaled enterprise cyber capabilities—from founding the Red Team to instituting an executive-facing metrics program and maturing control health across large application/product portfolios—so leaders could prioritize spend, brief regulators/boards with confidence, and ship safely at scale in a global, regulated environment (including seven-figure program scope).

Key Achievements (combined)

- Made risk decision-ready for executives and regulators by unifying 40+ KRIs/KPIs across 12 domains (IAM, TVM, IR, TPRM, Cloud) with clear ownership and data lineage—ending metric disputes and enabling apples-to-apples trend analysis.
- Managed ~300+ applications across 25 products within Chase Home Lending & Auto Finance, building tight partnerships with development leaders and proactively gathering control/architectural details—reducing late-stage surprises and waiver churn.
- Improved remediation flow and time-to-green by introducing product-line scorecards, risk councils, and accountable tracking that aligned remediation sequencing with business impact.
- Founded and industrialized the enterprise Red Team (charter, ROE, safety controls, integration with IR/SOC/risk) and executed 12+ full kill-chain simulations—turning testing into an executive input rather than a one-off activity.
- Closed the loop with purple teaming to convert findings into tuned detections, tabletops, and hardened reference patterns—shifting left so vulnerabilities were prevented, not just found.

Key Results (combined)

- Cleaner regulatory exams (e.g., OCC/FFIEC) with fewer follow-ups, driven by consistent metrics and traceable evidence.
- Reduced late-stage surprises and waiver churn across the Home Lending & Auto Finance portfolios.
- Improved time-to-green on prioritized control gaps through transparent scorecards and sponsor-backed sequencing.
- Reduced pre-launch criticals on services touched by red-team campaigns and faster remediation via integrated backlogs/CI/CD.
- Higher true-positive rates and better containment/dwell-time metrics following purple-team detection tuning.
- Executive dashboards adopted as the authoritative view, enabling confident quarterly board/regulator briefings and data-driven investment decisions.

Earlier Roles : Barclays — Vice President, Global Information Security | **KPMG —** Manager, Information Risk Assessment | **Citigroup —** Technology Risk & Security Consultant | **Fischer International Systems —** Software Security Engineer

EDUCATION

- M.S., Computer Science & Information Security — University of North Carolina at Charlotte
- B.E., Computer Science — Government Engineering College, Aurangabad (India)

CERTIFICATIONS

CISSP • CISM • CIPP/US • AWS Certified Cloud Practitioner • GIAC GCIH • MIT Data Science & ML