Saniya Bhaladhare

saniyabhaladhare@gmail.com +1 425-667-3748 San Jose, CA linkedin.com/in/saniyb/ github.com/Sann0311

PROFESSIONAL SUMMARY

GRC and security professional with 2 years of experience across control assessments, risk remediation, policy development, and GRC tooling for 7 regulated financial institutions. Built Python/FastAPI compliance automation across 227 controls, implemented RSA Archer workflows, and developed risk registers and remediation tracking used across regulated environments.

WORK EXPERIENCE

AI Security Engineer Intern, *Avaly.AI* 06/2025 – 08/2025 | United States

- **Reduced manual audit effort approx. 20% across 227 controls:** architected a Python/FastAPI compliance automation tool containerized with Docker and deployed via GitHub Actions CI/CD, automating control checks and evidence workflows across NIST AI RMF and ISO/IEC 42001.
- **Standardized GenAI vendor assessment across 7 trustworthiness domains:** designed a repeatable self-assessment covering risk scoring, evidence validation, and control traceability, becoming the standard governance process for new vendor onboarding.
- **Surfaced 10+ AI abuse cases and shipped 12+ safeguards:** threat-modeled 5 core workflow stages of a production LLM compliance agent, uncovering prompt injection, evidence tampering, and sensitive data exposure, and mapped findings directly to NIST AI RMF controls.
- **Facilitated 2 tabletop exercises surfacing escalation and response gaps:** ran AI incident simulations with product and engineering stakeholders, sharpening escalation paths, response ownership, and governance controls across high-risk LLM audit scenarios.

Cybersecurity Analyst, *KPMG* 01/2023 – 07/2024 | India

- **Elevated control maturity from 2.5 to 3.8 ahead of supervisory review:** identified 80+ control gaps across a large-bank cybersecurity maturity assessment and drove targeted remediation against NIST CSF and ISO 27001, producing a roadmap that became the institution's baseline for ongoing control governance.
- **Deployed RSA Archer GRC across 2 regulated institutions:** configured assessment templates and remediation workflows, tracked observation closure, and generated auditable risk reporting records used across ongoing governance cycles.
- **Deployed remediation dashboards and risk registers across 7 regulated institutions:** designed tracking frameworks that became each client's primary mechanism for monitoring control gaps, owners, remediation milestones, and observation closure across quarterly governance cycles.
- **Tested SDLC and change management controls across 4 engagements:** executed 20+ control tests covering code changes, deployment approvals, and release governance, surfacing 8+ observations incorporated into client remediation plans.
- **Reviewed Active Directory and IAM configurations across 5 environments:** examined user provisioning, group policy, access reviews, and privileged access governance, surfacing 10+ identity and access-control gaps incorporated into remediation.
- **Evaluated third-party security risk across regulated environments:** reviewed vendor security practices, contract security requirements, cloud controls across AWS, Azure, and GCP, and subprocessor risk posture, producing prioritized findings for client remediation.
- **Authored 5 enterprise policies accepted at CISO level:** owned Asset Management, Change Management, BCP/DR, Security Awareness, and Tabletop Exercise documentation, maintaining review cycles used for ongoing supervisory readiness.

TECHNICAL SKILLS

GRC & Compliance: SOC 2, ISO 27001, ISO/IEC 42001, NIST CSF, NIST RMF, NIST 800-53, PCI DSS, GDPR, ITGC, TPRM, Vendor Risk, Risk Register Management, Control Testing, Issue Management, Residual Risk Assessment, Policy Development, Tabletop Exercises, Executive Reporting

GRC Platforms: RSA Archer GRC, ServiceNow, Vanta

Automation & Engineering: Python, FastAPI, GitHub Actions, Docker, SQL

Cloud & IAM: AWS, Azure, GCP Security Evaluation, IAM Configuration Review, Active Directory, Access Reviews, Cloud Misconfiguration Analysis

AI Governance: NIST AI RMF, ISO/IEC 42001, OWASP LLM Top 10, AI Threat Modeling, LLM Audit Automation, GenAI Vendor Assessment, EU AI Act

EDUCATION

M.S. Cybersecurity Engineering, *University of Washington Bothell | GPA: 3.7/4* 09/2024 – 06/2026 | Bothell

B.Tech, Information Technology, *SNDT Women's University, Mumbai | GPA: 3.54/4.0* 08/2019 – 05/2023 | Mumbai

PROJECTS & LEADERSHIP

M.S. Thesis, *AI Compliance Framework for LLM Deployments* 09/2025 – 06/2026

- **Designed a 30-control framework cross-mapped across NIST AI RMF, ISO/IEC 42001, and OWASP LLM Top 10:** anchored a 0–5 maturity model to NIST SP 800-53A evidence hierarchy, eliminating duplicate evidence collection across overlapping frameworks.

SecurePipe , *DevSecOps CI/CD Security Pipeline* 03/2026

- **Caught 16 CVEs and 2 HIGH-severity vulnerabilities before deployment:** built a GitHub Actions pipeline with merge-blocking security gates using Bandit for SAST, Semgrep, pip-audit for SCA, and OWASP ZAP for DAST, remediating all identified findings to zero.

President, Women in Cybersecurity (WiCyS), *UW Bothell Student Chapter* 08/2025 – 06/2026

- **Grew chapter membership from 60 to 80 while leading an 8-member team:** delivered CTF nights, resume workshops, industry speaker panels, and certification sessions, building a recurring pipeline of hands-on cybersecurity programming.

CERTIFICATIONS & ACHIEVEMENTS

Certifications: CompTIA Security+ | ISO/IEC 27001 Associate | CISA (Exam Scheduled October 2026) | Multi-Cloud Red Team Analyst, Cyberwarfare Labs | EC-Council: Network Defense Essentials, Ethical Hacking Essentials.

Achievement: CTF Winner - UWB GreyHats (OSINT, cryptography, web exploitation, reverse engineering)

Thought Leadership: Research paper on compliance engineering for LLM systems under peer review at ICSE 2027 | medium.com/@saniyabhaladhare , on AI security and LLM threat modeling.