

Saniya Bhaladhare

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

PROFESSIONAL SUMMARY

GRC and AI governance professional with 2 years across compliance, third-party risk, and customer security assurance at 7 regulated institutions. Drove control maturity 2.5 to 3.8 at KPMG, and ships the automation behind the process: a Python/FastAPI audit agent operationalizing 227 controls, and a published 30-control AI compliance framework validated at 81.1% agreement with human assessors.

WORK EXPERIENCE

AI Security Engineer Intern, Avaly.AI

06/2025 – 08/2025 | United States

- **Cut manual audit effort approx. 20% across 227 controls:** built a Python/FastAPI audit agent, Dockerized and deployed via GitHub Actions, automating control validation against 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, adopted as the company standard for vendor and subprocessor onboarding.
- **Surfaced 10+ AI risk vectors and shipped 12+ safeguards:** threat-modeled 5 workflow stages against the OWASP LLM Top 10, uncovering prompt injection, evidence tampering, and data exposure, with mitigations adopted as engineering controls.
- **Ran 2 AI incident tabletop exercises** with product and engineering, sharpening escalation paths and response ownership across high-risk scenarios.

Cybersecurity Analyst, KPMG

01/2023 – 07/2024 | India

- **Elevated control maturity 2.5 to 3.8 ahead of external audit:** identified 80+ gaps through interviews, documentation review, and control testing against SOC 1/SOC 2, ISO 27001, NIST CSF, and PCI DSS, producing the remediation roadmap adopted as the institution's governance baseline.
- **Owned security questionnaire responses and customer assurance documentation across 7 engagements:** validated control evidence across teams and represented security posture to external stakeholders under tight deadlines.
- **Ran TPRM and vendor security assessments:** scoped pre-assessments, reviewed vendor practices and contract security addenda, assessed subprocessor risk and cloud control design across AWS, Azure, and GCP, and drove remediation to closure.
- **Prepared 35+ audit workpapers in RSA Archer GRC:** documented testing procedures, evidence, and risk observations, and deployed Archer assessment and remediation workflows at 2 institutions.
- **Authored 5 enterprise policies accepted at CISO level:** Asset Management, Change Management, BCP/DR, Security Awareness, and Tabletop Exercises, maintained through review cycles referenced in later audits.
- **Tested ITGC, SDLC, and change management controls across 4 engagements:** executed 20+ tests on change authorization, segregation of duties, and release governance, surfacing 8+ observations.
- **Reviewed IAM and Active Directory across 5 environments:** examined provisioning, group policy, access reviews, and privileged access, surfacing 10+ identity control gaps.

CORE COMPETENCIES

GRC & Compliance: SOC 1/SOC 2 Type II, ISO 27001, NIST CSF, NIST 800-53, PCI DSS, HIPAA, GDPR, ITGC, control testing, risk registers, policy development, audit readiness

AI Governance: NIST AI RMF, ISO/IEC 42001, OWASP LLM Top 10, EU AI Act, AI threat modeling, LLM audit automation, GenAI vendor assessment

Third-Party Risk & Customer Trust: TPRM, vendor security reviews, contract security review, subprocessor risk, security questionnaires, customer due diligence, evidence validation

Automation & Engineering: Python, FastAPI, GitHub Actions, Docker, CI/CD security, SAST/DAST/SCA, SQL

Cloud & Platforms: AWS, Azure, GCP security evaluation, IAM and Active Directory review, RSA Archer GRC, ServiceNow, Vanta.

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,** with a 0 to 5 maturity model anchored to the NIST SP 800-53A evidence hierarchy.
- **Validated AI-assisted assessment at 81.1% agreement with human assessors** against a 72.2% inter-assessor baseline. Extended version under review at ICSE 2027.

SecurePipe , DevSecOps CI/CD Security Pipeline

03/2026

- **Built a GitHub Actions pipeline with merge-blocking security gates:** integrated Bandit, Semgrep, pip-audit, and OWASP ZAP, catching 16 CVEs and 2 HIGH-severity vulnerabilities pre-deployment and remediating all to zero.

HIPAA Security Rule Readiness Assessment ,

06/2026

MyCarePortal - University of Washington

- **Assessed 12 threats across administrative, physical, and technical safeguards:** built a Streamlit dashboard scoring control readiness with exportable compliance reporting.

President, Women in Cybersecurity (WiCyS), UW Bothell Student Chapter

08/2025 – 06/2026

- **Grew membership 60 to 80 leading an 8-member team:** CTF nights, resume workshops, and industry speaker panels.

CERTIFICATIONS & ACHIEVEMENTS

Certifications: CompTIA Security+ | ISO/IEC 27001 Associate | CISA (Exam Scheduled October 2026) | AWS Certified AI Practitioner (In Progress) | 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.