

Bhavya Tiwary

hi@bhavyatiwary.com | bhavyatiwary.com | LinkedIn | Credly

Skills

Security Specific: Technical risk assessments, Architecture Reviews, Third Party Risk Management, AI/ML Lifecycle Security- Responsible AI, BC/DR, SOC 2 Type I/II/III, NIST AI RMF 1.0, NIST 800-39, ISO 27001, Cloud Security, Hardening Guidelines, Policy Development

Platforms and Languages : AWS, Azure, Prisma-CNAPP, Qualys CSPM, Git, GitHub Actions, Power BI, Entra ID (Graph APIs), Qualys CASB, Zcaler CASB, Archer GRC, CyberArk, Python (Automation), Bash

Experience

Infosys Ltd. (Information Security Group- Security Architecture)

Information Security Analyst

July 2024 – Present

- Developed the AI Security and Governance framework for the organization with stakeholders from various teams like Responsible AI, Legal, DPO etc
- Implemented ShadowAI CASB policy for sites providing AI services as part of ShadowIT initiatives to reduce data leakage risk and phishing attack risk.
- Conducted architecture and firewall rule-base review for internal platforms that leverage open source models for facial recognition and IoT sensor-based detection to improve physical security for data centers and offices.
- Assisted in the evaluation of new security controls such as DAM (Database Access Management) and Agentic SOC solution (Simbian).

Senior Information Security Engineer

July 2023 – July 2024

- Supported the team to demonstrate the organization's adherence to controls under the security and governance for the ISO 42001:2023 audit
- On-boarded Palo Alto's Prisma CNAPP tool to enhance company's cloud security governance posture. As part of the configuration process, established the cloud baseline controls for AWS, Azure and GCP cloud services; driving the development and ongoing improvement of the enterprise-wide cloud security architecture program
- Collaborated with RAI stakeholders to evaluate tools for AI Security. These tools covered governance (IBM WatsonX) as well as LLM- specific security (HiddenLayer, AIShield etc).
- Identified security and process gaps as well as implement enhancements for platforms like IBM WatsonX AIMS portal, RSA Archer GRC portal, SeriveNow etc that were used for BAU tasks

Information Security Engineer

August 2021 – July 2023

- Conducted third-party risk assessments to assess compliance with industry security standards like ISO 27001, SOC etc and architecture review to ensure secure setup on organization's physical datacenter and cloud workloads
- Reviewed and updated the business continuity and disaster recovery plan for business-critical services like AD and SIEM including data protection and security solutions for backup storage
- Assessed the shared mailbox usage to implement fine-grained access control and ultimately automating the process to reduce manual effort by 60

Certifications

Certified Information Systems Security Professional (CISSP) [Link](#)

Nov, 2025 - Oct, 2028

CompTIA Security +ce (SY-601) [Link](#)

June 2023 - June 2026

Microsoft Certified: Azure Fundamentals (AZ 900) [Link](#)

Education

MIT World Peace University, Pune

July 2021

B Tech - Computer Science and Engineering