MUHAMMED ASLAM CB

Enterprise Security Architect | Zero Trust & Multi-Cloud Security | vCISO / Fractional Security Advisory

aslamcb@gmail.com · +91 98954 01048 · Kerala, India (Remote-Global) · linkedin.com/in/aslamcb · aslamcb.com

TOGAF 10 · CISSP · CISM · CCZT

PROFESSIONAL SUMMARY

Strategic cybersecurity and enterprise security architect with 15+ years of progressive experience (12+ years focused on security architecture) designing and governing security for large, complex, multi-business-unit organizations across regulated healthcare, banking, insurance, telecommunications, and retail/conglomerate environments spanning the Middle East, Australia, the United States, Europe, and Asia-Pacific. Currently serves as security architecture design authority across a federated, multi-operating-company group, partnering with a dedicated security officer in each business unit to align controls and risk appetite. Proven track record leading Zero Trust and multi-cloud (AWS, Azure, GCP) transformation with zero security incidents across large-scale migration programs, architecting security for 100+ enterprise applications, and influencing $500K+ in security technology investment. Owns application security governance using industry-standard SAST/DAST/SCA and vulnerability-management tooling as mandatory design and pre-production gates, backed by penetration-test sign-off. TOGAF-certified for enterprise architecture and ADM-driven governance, and SABSA-grounded for risk-driven, business-attribute-led security architecture — translating board-level strategy into defensible controls and engineering guardrails. Current focus areas include AI & AI Agentic Security (agent identity, tool-use risk, MCP governance) and Zero Trust across distributed multi-cloud estates. Advises CISOs, CIOs, and boards as a trusted outsourced security leader on strategy, risk appetite, architecture governance, and audit/regulatory readiness.

CORE COMPETENCIES

Zero Trust Architecture · TOGAF Enterprise Architecture · SABSA Security Architecture · AI & AI Agentic Security · Multi-Cloud Security (AWS/Azure/GCP) · vCISO & Security Leadership Advisory · Application Security Governance · Identity & Access Management · Architecture Governance (CAB/EARB) · Data Protection & Classification · Compliance (SOC 2/ISO 27001/HIPAA/GDPR/PCI-DSS) · Board & C-Suite Risk Communication

PROFESSIONAL EXPERIENCE

Security Architect — 2026 — Present

Global Multi-Opco Retail, Real Estate & Entertainment Conglomerate · UAE (Remote)

- Act as security architecture design authority across a multi-Opco, parent–subsidiary group spanning retail, real estate, and entertainment, partnering with a dedicated Business Information Security Officer in each operating company under a federated governance model.
- Architect and approve security designs for major cloud transformation programs on Azure and AWS landing zones, including a hyperconverged-infrastructure migration and group-wide data center network modernization.
- Own application security architecture governance across the SDLC — SAST/DAST/SCA and vulnerability-management platforms as mandatory design and pre-production gates, backed by VAPT sign-off.
- Maintain a defense-in-depth control library spanning identity, API, data, network, endpoint, mobile, AI, and third-party-risk domains — the reference standard for every architecture review board submission.
- Design identity and access architecture (SSO/MFA/Conditional Access, privileged access management) and network/application-edge defenses (WAF/DDoS, API gateway) across cloud and on-premise estates.
- Lead security architecture reviews for GenAI and agentic-AI adoption — enterprise LLM agents and an AI-agent-to-ERP integration proof of concept — applying zero trust and least privilege to novel architectures.
- Apply TOGAF and SABSA to build reusable “standard architecture” patterns for repeat project types, reducing bespoke security review cycles across the group.

Cybersecurity Architect — 2022 — 2026

Global Telecommunications & Financial Services Technology Provider

- Served as security design authority providing group-level security architecture leadership across infrastructure, platforms, and multi-cloud environments (AWS, Azure, GCP) for global telecommunications and financial-services clients.
- Defined and maintained security architecture standards, reusable patterns, and blueprints — cloud landing zones, identity architecture, centralized logging, and encryption strategies — across 100+ enterprise applications.
- Operated a risk-based, iterative security architecture review model integrated into agile delivery; defined, tracked, and reported architecture KPIs including review cycle time, exception trends, and pattern adoption.
- Translated regulatory requirements (SOC 2, ISO 27001, HIPAA, PCI-DSS) into technical architecture standards; influenced CIO/CISO stakeholders through architecture review board presentations, and mentored security architects and application security engineers.

Cloud Solution Architect — 2019 — 2022

Global IT Services & Consulting Firm · Healthcare Client Engagement, Australia

- Architected enterprise-wide infrastructure and application security for a major healthcare organization supporting 17,400+ users in a highly regulated environment, achieving zero security incidents across the full cloud migration

program.

- Owned security architecture approval for EMR, patient engagement, and clinical application modernization; designed secure Azure landing zones and defined the shared-responsibility model across provider, platform, and application teams.
- Established application security frameworks covering OWASP Top 10 mitigations, secure coding standards, and authentication/authorization patterns, integrated with agile sprint cycles.
- Designed secure integration patterns for healthcare data exchange, ensuring controlled data flows, encryption, audit trails, and regulatory compliance (SOC 2, ISO 27001).

Senior Infrastructure Consultant & Technical Lead — 2010 — 2019

Pan-UK Education Technology & Managed Services Provider · 100+ Institutions

- Provided security architecture leadership for 100+ UK educational institutions under strict GDPR compliance, establishing reference designs for network security, endpoint security, and data protection.
- Designed secure hybrid-cloud architecture integrating on-premise Active Directory with Azure AD, and applied Zero Trust principles — device compliance, conditional access, identity-based controls — across a large, distributed multi-tenant estate.
- Implemented data classification frameworks and encryption strategies for sensitive student and staff information; led security architecture reviews for cloud migration and data center consolidation initiatives.
- Recognized with the “Outstanding Achiever of the Year” award (2017) for leadership in delivering secure infrastructure architecture across a distributed, multi-site environment.

IT Infrastructure Engineer — 2009 — 2010

Multi-Site Business Process Outsourcing Provider · Australia & India

- Designed security architecture for multi-site BPO infrastructure spanning Australia and India, including cross-border connectivity, zone-based network segmentation, and encryption for data in transit and at rest.
- Designed access-control architecture using Active Directory (role-based access, privileged access controls) and conducted security architecture assessments for infrastructure projects.

TECHNICAL EXPERTISE

Cloud Security	AWS IAM, GuardDuty, Security Hub, KMS · Azure Sentinel, Key Vault, Defender, Entra ID · GCP
Identity & Access	Entra ID, Okta, Ping Identity, CyberArk PAM, HashiCorp Vault, SSO/MFA/Conditional Access
SIEM/SOAR	Splunk, IBM QRadar, Microsoft Sentinel
Data Protection	DLP, CASB/CSPM, Key Management, Data Classification, Cross-Border Data Flows
EDR/XDR	CrowdStrike Falcon, Microsoft Defender, SentinelOne
Network Security	WAF/DDoS, API Gateway, VPN/ZTNA, Palo Alto, Cisco ASA, Fortinet
Application Security	Checkmarx, Burp Suite, OWASP ZAP, Snyk, SAST/DAST/SCA, VAPT Sign-off
Governance & Frameworks	TOGAF ADM, SABSA, NIST CSF/800-53, MITRE ATT&CK, CAB/EARB
AI & Emerging Tech	GenAI/Agentic AI Security, Copilot & Azure OpenAI Governance, LLM-Agent/MCP Security
Infrastructure	VMware, Hyper-V, Nutanix HCI, Active Directory, Hybrid Cloud

CERTIFICATIONS

CISSP — ISC² · CISM — ISACA · TOGAF 9/10 Certified — Enterprise Architect, The Open Group · CCZT — Certificate of Competence in Zero Trust, Cloud Security Alliance · SABSA Foundation (training complete, methodology applied in practice) · Microsoft Certified: Cybersecurity Architect Expert (SC-100) · Microsoft Certified: Azure Solutions Architect Expert (AZ-305) · Microsoft Certified: Identity and Access Administrator Associate (SC-300) · Microsoft Certified: Azure Administrator Associate (AZ-104) · AWS Certified Solutions Architect — Associate · Red Hat Certified Engineer (RHCE) · ITIL v3 Foundation — AXELOS

EDUCATION

Bachelor of Science, Electronics — MES College, MG University, Kerala, India (2007)

ENGAGEMENT FOCUS

Zero Trust & cloud security architecture reviews · SOC 2/ISO 27001/HIPAA readiness programs · AI & agentic system security assessments · Fractional CISO/vCISO retainers

Company names withheld by design — engagement context, scope, and outcomes are represented accurately above. References and verifiable details available on request.