Kotaiba Alhaj

Director of GRC | Visalia, CA | 714-724-0714 | kotaiba.alhaj2@gmail.com | linkedin.com/in/kotaibaalhaj

Director of GRC Highlight Reel

Security & GRC Leader with extensive experience in building and leading enterprise ISMS/GRC programs, driving security maturity initiatives, and operationalizing audit readiness for external certifications.

• Built & led an enterprise ISMS/GRC program across a regional municipality, cutting measured risk exposure ~75%, sustaining multi-cycle ISO 27001 certification, and aligning to NIST.
• Drove 60+ security maturity initiatives and 50+ assessments; reduced incident response times ~50%, and compressed RTO from 10 days to 60 minutes with tested BCP/DR.
• Established an enterprise risk management framework and operating rhythm (risk taxonomy, risk registry, KRI/KPI dashboards), enabling executive and Audit Committee reporting.
• Operationalized audit readiness for external certifications—evidence mapping, owners, and cadence—resulting in faster closes and 200%+ improvement in audit preparedness.
• Recognized for program excellence (Top 50 CISOs, Ajman Excellence) and for raising citizen trust scores to >90% through secure digital services.

Experience

Paramount Computer Systems (Cybersecurity consultancy) — **California / Remote**

Program Lead, Cybersecurity Governance, Risk & Compliance — 2016 - Present

- Owned the end-to-end GRC program for a large public-sector enterprise: policies/standards, risk, compliance, privacy alignment, third-party governance, and audit readiness.
- Designed and ran the ERM lifecycle: workshops, risk scoring, risk registry upkeep, mitigation tracking, and quarterly leadership/Audit Committee reporting; improved closure rate on high risks by >60%.
- Led SOC 2/HIPAA/SOX-ITGC readiness efforts (control mapping, evidence calendars, walkthroughs, sampling, issues mgmt); completed 3 ISO certification cycles (27001/20000/22301).
- Implemented continuous control monitoring and evidence automation via a Trust/GRC platform (Vanta-equivalent), integrated with ticketing/IDP; cut manual evidence collection ~40% and shortened auditor requests ~30%.
- Directed two 3-year security roadmaps; shipped 60+ initiatives (IR playbooks, BIA, DR tests, secure SDLC checkpoints, awareness campaigns), contributing to 6/7 digital-services rating.
- Built a federated governance model with policy owners across Security, IT, Product, Legal, HR, Finance; drove adoption via champions program, training, and KRIs/KPIs.

The Executive Council — Government of Dubai — **Dubai**

IT Executive (IT Operations & Security) — 2012 - 2016

- Delivered VIP-grade IT/security services; implemented ISMS/ITSM to achieve ISO 27001 & ISO 20000 compliance; increased service reliability and reduced Sev-1 MTTR.

Additional Consulting & Early Roles

Consultant — 2011 - 2023

- External auditor/assessor exposure with ISO 27001/20000/22301; program advisory to executive teams (GTM and security governance).
- Led field and IT teams for a city census covering ~500K residents; coordinated 50 staff across data collection and infrastructure.

Education

Al-Ain University of Science & Technology
B.S. | Networks & Communication Engineering
UAE

Certifications

ISO 27001/20000/22301/9001 Lead Auditor

ISO 31000 Risk Manager

COBIT 5 (Foundation/Assessor/Implementer)

ITIL

Managerial Leadership Diploma

Skills (Aledade-Aligned)

GRC & Risk: ERM · risk taxonomy · risk registry · KRIs/KPIs · issue mgmt · third-party risk · Audit Committee reporting

Compliance & Privacy: SOC 2 · HIPAA · SOX/ITGC · HITRUST · CPRA/CCPA · ISO 27001 · NIST · AI RMF · evidence frameworks · auditor coordination

Platforms & Tooling: Vanta · Trust Center · CCM · evidence automation · OneTrust · Archer · IDP/SIEM/MDM integrations · Ticketing · CMDB

Security Program: Policy/standard lifecycle · secure SDLC checkpoints · awareness & culture · BIA/BCP/DR (RTO/RPO) · IR playbooks · metrics & exec reporting

Leadership: Team Building · cross-functional influence · Vendor Management · roadmap & budget