Abdulla Juma Ali Belqaizi AlFalasi

Information Security Governance & Risk Management Professional

SUMMARY

Governance-focused Information Security professional with extensive experience in information security policy, cyber risk management, audit and compliance coordination, cloud and application security governance, data protection, and security assessment oversight across regulated enterprise environments. Background combines operational security understanding with a governance-first approach to strengthen risk visibility, audit readiness, policy compliance, stakeholder alignment, and defensible security decision-making. Particularly strong in roles requiring governance maturity, policy discipline, audit defensibility, and risk-based security oversight within government, regulated, and enterprise environments.

SKILLS

Security Strategy & Program Governance | Cyber Risk Management & Risk Register | ISO/IEC 27001 ISMS Implementation & Audits | Regulatory & Audit Readiness (UAE IAS) | Governance, Risk & Compliance (GRC) | Incident Response Lifecycle Management | Cloud Security Governance (Multi-Cloud) | Security Policy, Standards & Procedures | SOC Establishment & Managed Security Oversight | Executive Stakeholder & Board Communication | Vulnerability & Threat Management | Security Awareness & Culture Programs | Application & DevSecOps Security Governance | Budget Planning & Security Investment Oversight | Data Protection & DLP Governance | Access Control & Identity Governance | SIEM | Threat Hunting | Firewall Management | Email Security | Endpoint Security | ITIL Framework

EXPERIENCE

Information Security Policies Specialist — Abu Dhabi Housing Authority

Dec 2019 – Present • Abu Dhabi, UAE

Led information security governance across a UAE government authority, effectively functioning at section-head level with full accountability for budget management, resource coordination, departmental planning, KPI ownership, and operational execution. Directed enterprise-wide security program including ISO 27001 ISMS certification, regulatory compliance audits, risk register ownership, SOC establishment, multi-cloud security governance, and security review/approval authority over all technology changes and deployments. Drove strategic security investments including DLP, GRC platform, NDR, and cloud security capabilities while building team capability and maintaining continuous audit readiness.

- • Assumed section-level leadership responsibilities encompassing budget management, resource coordination, departmental planning, KPI ownership, and operational execution — effectively functioning as Information Security Section Head
- • Led dedicated security team, overseeing task delegation, performance development, capability building, and continuous alignment with enterprise GRC objectives
- • Governed security review and approval of all new solutions, infrastructure changes, application enhancements, and technology deployments prior to production — enforcing security-by-design philosophy organization-wide
- • Spearheaded information security risk management by owning the risk register, driving risk treatment actions, and ensuring residual risk remained within executive-approved thresholds
- • Supported governance discussions for emerging AI/data use cases, establishing ownership models, role clarity, and operational governance structures before business adoption
- • Led end-to-end planning and coordination of ISO/IEC 27001 surveillance and recertification audits — including evidence collection, cross-functional stakeholder engagement, audit response, and closure of corrective actions, achieving continued certification
- • Developed, reviewed, and continuously enhanced organization's information security policies, standards, and procedures to mature ISMS compliance with ISO 27001, ISO 20000, and UAE cybersecurity regulatory requirements
- • Coordinated regulatory compliance audits by reviewing security controls, assembling required evidence packages, and tracking remediation to closure — maintaining defensible, audit-ready security posture
- • Delivered KPI performance targets for Information Security Section, including maintaining 90%+ incident closure within defined SLAs
- • Established and operationalized 24/7 SOC providing SIEM-based monitoring, threat detection, and security event triage — building organization's first managed security monitoring capability
- • Governed security across two multi-cloud environments, conducting cloud infrastructure security audits and delivering risk-based observations and remediation recommendations aligned to cloud security best practices
- • Directed application security governance including Web, Mobile, and Source-Code Analysis reviews integrated into CI/CD-supported development and change lifecycles
- • Drove implementation of enterprise DLP, centralized GRC platform, NDR, and cloud security review capabilities — planning and influencing budget allocation to enable strategic security investments
- • Developed minimum security baseline requirements for applications and operating systems, reducing configuration drift and establishing consistent control standards across environment
- • Supported vulnerability assessment and VAPT activities across enterprise assets, applications, and cloud workloads
- • Led incident response lifecycle activities including detection, containment, eradication, recovery, and post-incident communication and reporting
- • Nominated to Data Management Team to provide information security input on data classification, privacy controls, and governance alignment — contributing to organization's Data Management Standard compliance

- Designed and delivered security awareness programs including workshops, advisories, and campaigns that measurably improved employee security behavior and organizational security culture
- Contributed to production security governance by enforcing segregation of access, ownership clarity, and restrictions on cross-team data visibility

IT Security Professional (SOC) — Injazat Data Systems

Jun 2016 – Dec 2019 • Abu Dhabi, UAE

Delivered multi-client security operations and managed security services across 17 concurrent enterprise client environments. Performed SIEM monitoring, incident response, threat hunting, vulnerability scanning, and security infrastructure management including firewalls, email security gateways, secure web appliances, and endpoint security platforms. Provided technical threat intelligence through proactive hunting activities and detailed threat reporting, supporting client security teams with actionable security insights and posture management aligned to client security policies.

- Monitored SIEM environments for security events and alerts; executed incident response procedures, phishing analysis, and technical threat reporting across multiple enterprise clients
- Conducted proactive threat hunting and prepared detailed technical threat reports, supporting client security teams with actionable intelligence
- Performed vulnerability scanning and security control tuning against client security policies, managing security posture across 17 concurrent client environments
- Operated and supported security infrastructure including Firewall Rules & Routing, Email Security Gateways, Secure Web Appliances, and Endpoint Security platforms
- Supported multi-client security operations: incident response coordination, log analysis across security appliances, and escalation management

Service Desk Analyst — Injazat Data Systems

Jun 2016 – Jan 2018 • Abu Dhabi, UAE

Provided Level 1 IT support and incident management services for multiple enterprise clients following ITIL framework processes. Delivered quality service delivery through structured incident management, knowledge management, and quality management practices across diverse client technology environments.

- Delivered Level 1 IT support and incident management for multiple enterprise clients, applying ITIL framework processes for incident, knowledge, and quality management

EDUCATION

Bachelor of Science, Computer Engineering (Minor: Electrical Engineering) — Marquette University

Aug 2010 – Jun 2015

CERTIFICATIONS

Certified Ethical Hacker (CEH)

EC-Council

CCNA Security (IINS)

Cisco

ITIL Foundation
AXELOS

CISSP (Training Completed)
ISC2

PEN-200 (OSCP) (Training Completed)
Offensive Security

SANS 560 (GPEN) (Training Completed)
SANS Institute

PMP (Training Completed)
PMI