

ANUGYA SARRASWAT

Head of Information Security ► Risk Group

Banking & Financial Services • Cyber Security • Technology Risk • Regulatory Governance

Doha, Qatar ► +974 7441 1121 ► anugya.s@gmail.com ► LinkedIn: /in/anugya-sarraswat

EXECUTIVE PROFILE

Senior Information Security leader with 17+ years in **banking cyber security, technology risk, and regulatory governance** — currently heading the Information Security function at Qatar Islamic Bank under the Risk Group as an independent **Second Line of Defense**. Built the function from inception over **eleven years at QIB across four promotions** — Specialist → Manager → Senior Manager → Head — earning deep institutional trust across Risk, IT, and the Board.

Trusted advisor to the Board and regulators; regular presenter to the **Operational Risk Management Committee (ORMC) and Board Audit & Risk Committee**. Active national-level voice in cyber security with QCB and sectoral authorities. Proven at **maintaining zero major cyber incidents through heightened geopolitical risk** and building security teams that retain talent and deliver under pressure.

WHY THIS LEADER ► Crisis-Tested. Resilience Architect. Secure Cloud Strategist. Trusted Board Voice.

Crisis Leadership ► Demonstrated cyber leadership during heightened Gulf geopolitical tensions — state-sponsored threats, DDoS campaigns, phishing surges, and remote-access risk. Validated end-to-end controls across network, endpoint, email, mobile, and SWIFT; enforced QCB-aligned VPN governance and real-time SOC/threat-intel integration. **Outcome: zero successful cyber-attacks and uninterrupted banking operations.**

Cyber Recovery & Out-of-Country DR ► Drafted and executed the bank's end-to-end Cyber Recovery solution (Dell/GBM) — designed the out-of-country DR security strategy from the ground up, ensuring **data integrity, environment isolation, and secure cross-site replication**; defined data-at-rest and data-in-transit controls, DR access governance, and BCM-aligned recovery assurance testing.

Secure Cloud Adoption Strategy ► Governed phased cloud adoption (Azure, SaaS) with QCB-aligned risk assessments, Zero Trust principles, and regulatory-compliant cloud exit strategy; led **Windows 365 Cloud Remote Desktop** project security end-to-end — endpoint policy, identity integration, network segmentation, conditional access, and secure data boundary controls.

LEADERSHIP TRAITS ► Decisive Under Pressure ▪ Builds & Retains Top Talent ▪ Board-Credible Communicator ▪ Independent & Principled ▪ Long-Tenured & Trusted

SIGNATURE ACHIEVEMENTS AT A GLANCE

ZERO

Major Cyber Incidents
Through Crisis

11 yrs

At QIB
4 Promotions

15+

Security Professionals
Led & Mentored

22+

Critical Apps Assessed
Fully Remediated

CURRENT ROLE AT A GLANCE

Head of Information Security – Risk Group | Qatar Islamic Bank | Doha, Qatar | May 2015 – Present (11 years)

Career path at QIB: Specialist (2015) → Manager, Information Security (Mar 2020) → Sr. Manager, Information Security (Jul 2023) → Head of Information Security (Acting)

Mandate: Independent 2nd Line of Defense across all technology and cyber domains • **Team:** 15+ professionals (GRC, SOC, App/Infra Security, Data Privacy) • **Reporting:** Risk Group Head; ORMC & Board Audit & Risk Committee

CAREER HISTORY — LONG-TENURED, BUILDER TRACK RECORD

Three roles across 18 years; deliberate long-tenure pattern reflecting commitment to building durable security functions and earning institutional trust rather than chasing titles.

Head of Information Security – Risk Group | Qatar Islamic Bank

May 2015 – Present

Doha, Qatar • 11 years • Specialist (2015) → Manager (Mar 2020) → Sr. Manager (Jul 2023) → Head of Information Security

- ▶ Lead the **Information Security function under the Risk Group** as Second Line of Defense, with independent control assurance and challenge across all technology and cyber domains; team of **15+ professionals** across GRC, SOC, Infrastructure & Application Security, and Data Privacy.
- ▶ Regular presenter to the **Operational Risk Management Committee (ORMC)** and **Board Audit & Risk Committee** — own the enterprise cyber risk narrative, KRI/KPI dashboards, and regulatory posture; **secured Board endorsement** for the multi-year Information Security Strategy & Roadmap (2025–2026).
- ▶ Active national-level engagement with **Qatar Central Bank (QCB)**, sectoral authorities, and peer CISOs; led the bank's **National Cyber Drill** participation (achieved '**Excellent**' rating), threat-intelligence exchange, and inter-bank cyber forums.
- ▶ **Crisis Leadership – Geopolitical Risk**: Validated end-to-end controls across network, endpoint, email, mobile, remote access, and SWIFT during heightened Gulf-region tensions; reinforced DDoS, WAF, and perimeter defences. **Outcome: zero successful cyber-attacks** during peak threat period.
- ▶ Led the bank-wide **Identity & Access Management transformation (SailPoint)** — joiner/mover/leaver automation, role mining, RBAC redesign, SoD controls, and access certification; integrated **Privileged Access Management** (jump-server, session recording, MFA) across critical infrastructure including **Temenos T24 core banking migration** with full security sign-off at every project gate.
- ▶ Led **QCB Technology Risk Circular** self-assessment and **QCB Data Protection 2026 readiness**, with clause-level mapping to NIST SP 800-53/61/207/218, PCI DSS, ISO 27001, CIS Controls, and CSA CCM.
- ▶ **Data Privacy Officer (DPO) oversight as Second Line of Defense** — the bank's DPO function reports under Information Security; responsible for **Qatar PDPPL** compliance, **GDPR** alignment, consent management, data subject rights fulfilment, privacy impact assessments (PIAs), and cross-border data transfer governance.
- ▶ Implemented **enterprise-wide data classification, DLP (Forcepoint), and database activity monitoring (IBM Guardium)**, with encryption and field-level masking; delivered **24x7 SOC and MDR transformation** (CrowdStrike, Exabeam CLM, LogRhythm) maturing detection engineering and threat-intel integration.
- ▶ **Cyber Recovery & Out-of-Country DR**: Drafted and executed the bank's **Cyber Recovery solution** (Dell/GBM) end-to-end — designed the **out-of-country DR security strategy**, ensuring data integrity, environment isolation, and secure replication across sites; defined security controls for data-at-rest and data-in-transit, access governance for DR environments, and recovery assurance testing aligned to BCM requirements.
- ▶ **Secure Cloud Adoption & Cloud Remote Desktop**: Governed phased cloud adoption (Azure, SaaS) with QCB-aligned risk assessments and cloud exit strategy; led the **Windows 365 Cloud Remote Desktop** project security — endpoint policy, identity integration, network segmentation, conditional access, and secure data boundary controls ensuring regulatory compliance throughout deployment.
- ▶ Owned **InfoSec budget planning, vendor selection, and RFP security evaluation** across 15+ enterprise security platforms; consistent ROI optimisation through strategic OEM partnerships.

Solution Architect & Engagement Manager | Atos

Jul 2010 – Apr 2015

India • Enterprise Security Solutions & Managed Services • ~5 years

- ▶ Architected and delivered **enterprise security solutions** for global BFSI, telecom, and government clients, leading multi-disciplinary engineering and consulting teams; led pre-sales and engagement management for large security RFPs.
- ▶ Designed **SIEM, IAM, endpoint, and network security architectures** with vendor-agnostic blueprints; oversaw deployment, integration, and managed-service transition.

Chief Security Officer | Telecanor Global Limited

Jul 2008 – Jun 2010

India • Enterprise Security Leadership • 2 years

- ▶ Held **CSO accountability** for enterprise security strategy, policy, operations, incident response, and vendor controls; built and led the security team from ground-up.

LEADERSHIP PHILOSOPHY & VALUE TO THE ORGANISATION

Building & Scaling Teams	Built the bank's Information Security function from inception to a 15+ professional, multi-domain organisation — recruiting, mentoring, and retaining top cyber talent.
Translating Risk to Business Value	Bridge the gap between technical depth and board-level decision-making — distil cyber risk into commercial impact and prioritised investment cases.
Regulator-Ready Posture	Audits, QCB inspections, and Board challenges met from a position of confidence — documented evidence, clause-level traceability, remediation already in motion.
Crisis Decision-Making	Calm, decisive leadership under pressure — proven through geopolitical crises, ransomware threats, and live incidents where the first hour matters most .

STRATEGIC PROGRAMS DELIVERED

SOC & MDR Transformation	24x7 detection on CrowdStrike, Exabeam CLM, LogRhythm • 'Excellent' rating in National Cyber Drill
IAM Lifecycle (SailPoint)	Bank-wide identity governance, RBAC redesign, SoD controls, PAM, MFA, access certification
DevSecOps (NIST 800-218)	Secure SDLC, SAST/DAST/SCA, API protection across Temenos T24 and digital channels
Cyber Recovery & Out-of-Country DR	Drafted & executed full Cyber Recovery solution (Dell/GBM) — out-of-country DR security strategy, data & environment integrity, secure replication, DR access governance, and BCM-aligned recovery assurance
QCB Data Protection 2026	Enterprise data classification, DLP, encryption, masking; clause-level PDPPL & QCB regulatory mapping
Secure Cloud & Cloud Remote Desktop	Azure / SaaS QCB-compliant adoption; Windows 365 Cloud Remote Desktop — endpoint policy, identity integration, conditional access, secure data boundary controls
Quantum-Safe Encryption	Post-quantum cryptography readiness — algorithm inventory (RSA/ECC exposure), NIST PQC migration roadmap (ML-KEM, ML-DSA), key lifecycle governance
AI Security & Guardrails	AI security governance — model risk controls, prompt injection defence , input/output validation, data protection in AI pipelines, and bias & integrity monitoring
PDPPL & GDPR — Privacy Governance	Data Privacy Officer (DPO) oversight as Second Line of Defense — Qatar PDPPL compliance, GDPR alignment, consent management framework, data subject rights, privacy impact assessments, and cross-border data transfer controls

TECHNOLOGY STACK & REGULATORY FRAMEWORKS

Security Operations: CrowdStrike MDR/EDR • Exabeam CLM • LogRhythm SIEM • Threat Intelligence | **Data Security:** IBM Guardium DAM • Forcepoint DLP • Encryption & Key Management • Data Rights Management

Application & Network: F5 WAF • IBM API Connect • Ooredoo DDoS • HIPS / App Whitelisting | **Identity & Cloud:** SailPoint IAM • PAM (Jump Server / MFA) • RBAC • Azure • Windows 365 • Defender Suite • MDM

Cyber Recovery & DR: Dell/GBM Cyber Recovery Solution • Out-of-Country DR • Secure Replication & Data Boundary Controls • BCM-Aligned Recovery Testing

Regulatory & Standards: QCB Technology Risk & Data Protection (2026) • Qatar **PDPPL** • **GDPR** • QCB Cloud Computing • NIST SP 800-53/61/207/218 • ISO 27001 • PCI DSS • CIS Controls • CSA CCM