Sanjay Jha

GRC Transformation Leader — IT, Security, Data Privacy, and Business Continuity.

Dubai, UAE +971-52-844-8269 skitgrc@gmail.com LinkedIn Profile

● CISA ● CISM ● CRISC ● CDPSE ● C|CISO ● CPISI ● ITIL ● ISO 27001 LI & LA ● ISO 9001 LA ●

1. Executive Profile

Extensive Leadership Experience: Sanjay is a science graduate (1989) and a visionary leader with decades of global work experience, including leadership roles within Governance, Risk Management, and Compliance (GRC).

Delivery-Oriented & Global Reach: Sanjay is a delivery-oriented professional with rich experience in a cross-border environment and has demonstrated his leadership values while servicing clients across America, Europe, Asia Pacific, and the Middle East, embracing challenges as opportunities for growth.

As a GRC transformation leader, Sanjay can add value to the following:

1) Establish or transform a **governance and risk management framework** to serve the board and executive members with an integrated view of enterprise risk exposure from three lines of defence perspectives.
2) Establish or transform an **information security function** based on the globally accepted frameworks.
3) Establish or transform a **data privacy function** based on the local and global data protection laws & regs.
4) Establish **Centre of Excellence (COE)** for security, privacy, governance, risk management, and compliance.
5) **Support merger and acquisition** by standardizing governance IT, cybersecurity, data privacy and BCP/DRP.
6) Establish the **management system** for ITSM, ISMS, BCMS, PIMS, and AI (AIMS – in progress).
7) Control **financial reporting risks** by building risk governance and oversight through **Internal Controls over Financial Reporting (ICFR)** using **IT General Controls (ITGC)** derived from COSO, COBIT, and NIST CSF.
8) Design a robust **risk control framework for service organizations** to assure the client organizations by using COSO, COBIT, ITGC, SSAE 18 /ISAE 3402 for SOC compliance readiness (SOC 1, Type 1 and Type 2).
9) Establish an **internal audit program** for IT, security, data privacy, and BCP using ITGC Controls.
10) Support executive management in **digital forensic investigations**.

2. Leadership Highlights

1) Demonstrated change leadership while supporting many Fortune 500 clients.
2) Established /transformed the Information Security and Data Privacy functions of many organizations.
3) Directed security & technology risk functions for clients across AG, EMEA, APAC, and Middle East.
4) Established Centre of Excellence (CoE) for Risk Management, SOX, and Business Continuity [Fortune 100].
5) Transformed the SOC operations, advanced threat intelligence practices, and cloud security frameworks.
6) Strong people leader: Built and scaled cross-border, multi-vendor teams, promoting collaboration across IT, Business Functions, Support Functions, and third-party service providers with a team of 125 members.
7) Known for building high-performing, accountable teams that drive innovation and operational excellence.

3. Key Skills

1) **Governance and Oversight:** Setting up Governance and Oversight for Information Technology, Security, Data Privacy, and Risk; and present KPI based risk posture, metrics, and remediation plans to the leadership.
2) **Strategic Cybersecurity & Privacy Leadership:**
   a) Develop Privacy Framework, Manage Privacy Program, Set up Data Privacy Practice.
   b) Align security and privacy strategies with corporate objectives to drive trust, resilience, and growth.
   c) **Cloud & Application Security:** Adopt secure-by-design architectures leveraging OWASP, CSA, and NIST frameworks for scalable cloud resilience.
3) **Technology Risk Management:**
   a) **Cross-Functional Collaboration:** Partner with Service Lines, HR, IT, Risk, Legal & Compliance to embed privacy/security-by-design principles.
   b) Oversee VAPT, red-team testing, SOC operations, and incident response.
   c) **Strategic Procurement & Emerging Tech Evaluation:** Lead proof-of-concepts and technology evaluations to adopt next-generation cybersecurity and privacy tools.
   d) **Vendor & Third-Party Risk Management:** Govern multi-vendor ecosystems & cross-border engagements with strong SLAs, compliance assurance, & due diligence.
4) **Regulatory compliance:** Proficiency in translating regulatory requirements into an actionable program.
5) **Audit and Assurance:**
   a) Oversee internal & external audits, and audit readiness.
6) **High-Performance Team Leadership:** Build, mentor, and inspire cohesive, outcome-driven security and privacy teams with accountability & innovation culture.

4. Professional Certifications

Certified Chief Information Security Officer	Certified Information Systems Auditor	Certified Information Security Manager	Certified in Risk and Information Systems Control	Certified Data Privacy Solutions Engineer	Certified Payment Card Industry Security Implementor
Certified ISO 27001 Lead Auditor	Certified ISO 9001 Lead Auditor	ITIL Certified IT Service Management	ACAMS Certified Anti-Money Laundering (Foundations)	ISACA Active Member	iapp Active Member

5. Executive Hiring Value Proposition | Value Offerings

Strengthening Enterprise Governance, Risk Management and Compliance for Security and Data Privacy.

By hiring this CISO & DPO capability, the organization secures a **strategic leader** who has capabilities to drive a unified digital risk governance around cybersecurity and data privacy, into a measurable business advantage which will result into a **protected, legally compliant, and resilient enterprise** where every control strengthens security, privacy and business continuity; every policy enhances customer trust and confidence; and every decision is a risk aware decision.

Below is an example of how hiring of this leadership capability can help the organization:

1) **Governance:**

   a) Establish Resilient IT, Security and Privacy Governance by defining policies/processes, objectives, roles and responsibilities, KPI and SLA using globally accepted frameworks such as COSO, COBIT, NIST CSF, etc. and ISO standards such as ISO 27001 (ISMS), ISO 27701 (PISM), ISO 20000 (ITSM), ISO 22301 (BCMS), and ISO 42001 (AIMS).

2) **Risk Management:**

   a) **Frameworks/Standards (implementation experience):** ISO 31000, ISO 27005, NIST CSF, COSO, and COBIT.

   b) **Technology Risk Management:** Establishes enterprise-wide technology risk controls with proactive vulnerability detection, patch governance, and quantifiable resilience reporting to the board.

   c) **Data Privacy Risk Management:**

      i) Data protection law & regulations were implemented by defining robust data privacy framework and executing a data privacy program to demonstrate organization's commitment towards compliance and building trust.

      ii) ISO 27701:2025 based Personal Information Management System (PIMS) was implemented to build trust.

   d) **IT Resiliency – Business Continuity & Disaster Recovery Planning:** Delivered ISO 22301-aligned continuity and recovery readiness, ensuring business operations remain uninterrupted under disruption.

   e) **Third-Party Risk Management – Outsourcing Risk:** Governs external vendors due diligence, Data Protection Assessments as per law, and continuous oversight to eliminate third-party risk exposure.

   f) **Digital Risk Management:**

      i) **Cybersecurity Risk Management:** Builds an adaptive, intelligence-driven cyber-defense capability that reduces breach likelihood and enhances response maturity.

      ii) **Cloud Security Risk Management:** Ensures secure, compliant cloud adoption through CASB integration, shared-responsibility models, and data-sovereignty assurance.

      iii) **Secure Digital Transformation:** Embeds security and privacy-by-design into digital initiatives, enabling innovation with control and compliance built in.

      iv) Support executive management in **digital forensic investigations**.

3) **Compliance**

   a) **Regulatory & Compliance Fulfilment:** Embeds legal & regulatory requirements into security and privacy operations to build trust and ensure anytime audit readiness and compliance with Data Protection Law, its Executive Regulation, UAE Information Assurance Regulation, SOX, SSAE 18, ISAE 3402.

   b) **Audit, Reviews and Assurance Excellence:** Maintains continuous audit readiness, for External and Internal Audits, and Gap Assessment, Readiness Review, Risk Controls Self-Assessments (RCSA), Peer Review, and Maturity Model Assessments of Security /Privacy Program.

   c) **Security and Privacy Assurance:** Creates a hardened security ecosystem safeguarding the IT landscape to have secured applications and data with 24×7 integrity and continuity.

6. Employment History

✍ KPMG Middle East [2024-2025]: Data Protection Officer (DPO)

Accountable for establishing and maintaining a resilient data privacy program aligned with the global and regional (Middle East) data protection laws and regulations.

My key responsibilities include regular collaboration with internal and external stakeholders in a cross-border environment, integrating data privacy requirements into business processes, and fostering a privacy culture within the organization.

Currently, I am playing a key role in building Governance around our Privacy Program using ISO 27701:2025, a framework for Personal Information Management System (PIMS).

The achievements:

1 Developed Data Privacy Framework based on Data Protection Laws & Regulations.

2 Institutionalized Data Privacy Program for UAE, Oman, KSA, Jordan, and Lebanon.

3 Institutionalized Resilient Privacy Governance.

4 Regulatory Compliance Preparedness and Oversight.

✍ KPMG Lower Gulf [2020-2024]: CISO and DPO

The achievements:

1 Institutionalized Cybersecurity Program to strengthen the Technology Risk Management.

2 Institutionalized Data Privacy Program in line with Data Protection Laws and Regulations in UAE and Oman.

3 Established Security & Privacy Governance in line with DIFC & ADGM data protection laws and regulations.

4 Obtained successful certifications /attestations for SOC 1 Type 1 and Type 2, ISO 27001 and ISO 9001.

5 Key initiatives during Covid-19 Pandemic Lockdown and Restrictions

- Deployed eSignature solution to overcome the challenges of physical signing of documents.
- Collaboration with other countries MF and arranged for local support for employees/secondees.
- Took initiative to deploy Virtual Desktop Infrastructure (VDI) to ensure business continuity during Covid19.

6 Improved the security culture and behavior among IT admins, employees, and vendor resources.

7 Managed the internal and external audits successfully and without any escalations or major findings.

✍ Dunia Finance [2015 –2019]: Head of Information Security | Head of IT Risk & Security

The achievements as Head of IT Risk and Security:

1 Established Technology and Cloud Security Risk Management Framework in line with UAE IA (NESA).

2 Established Secure Digital Transformation practice through Security by Design and Security by Default.

3 Optimized the Risk Controls Self-Assessment (RCSA) to meet the Central Bank of the UAE requirements.

4 Optimized the Security Operation Center (SOC) through advanced threat intelligence.

5 Strengthened the Vulnerability Management Program.

The achievements as Head of Information Security:

1 Established Information Security Management System and Governance in line with UAE IA (NESA).

2 Established security objectives, roles and responsibilities, KPI, SLA and initiated metrics-based evaluation of security controls effectiveness to strengthen the security governance and management reporting.

✍ IBM [Feb 2008 – Jan 2015]: EMEA Compliance Leader

Worked as **Compliance Leader** (GTS SARM: Technology Security and Risk Management) for EMEA regions. I was responsible to manage the Technology Security and Risk Management for 67 portfolios, 144 clients from 22 countries of EMEA region and manage the Technology Risk Management for a fortune 100 bank.

Sanjay achieved skills of collaboration in cross-border environment while managing technology security, risk and compliance for many of the Fortune 500 Multinational Banks and Financial institutions.

✍ Wipro Technologies [Jan 2006 – Feb 2008]: Program Manager

While being with Wipro, Sanjay extended his consulting services to the World Bank, CapitalOne, State Street. Sanjay also successfully established the Credit Suisse Center of Excellence (CoE) for Risk Management, SOX and BCP/DRP, supporting Credit Suisse across the USA, Canada, UK, and Singapore. While working with Wipro, As a short-term project, implemented BCMS based on ISO 23001:2006 standard for BMW Financial Services in Japan.

During his tenure with Wipro, he acquired the skillset of setting up the Risk Function as an entrepreneur.

✍ KPMG [Mar 2005 – Dec 2005]: Manager – Quality Registrar | Certification Auditor

Sanjay was responsible for the assessment of the design and operating effectiveness of Internal Controls implemented by banks and certifying them to be compliant with the regulatory requirements and with the Bank's Manual / Book of Instructions.

As a Certification Auditor for BS 7799 and ISO 9001, Sanjay was responsible for auditing and certifying Banking and Financial Institutions (Banking and Non-Banking) in India for their conformance to BS 7799 and ISO 9001.

During his tenure with KPMG, he acquired the entrepreneurial skills of managing accounts end-to-end.

✍ GTL Limited [Nov 2000 – Aug 2004]: Internal Auditor (Systems and Projects)

Internal Audit of information systems & sub-systems, data center operations, call center, BPO, and IT projects.

✍ Protolab Technologies [July 1993 – Nov 2000]: Business Application Developer.

Development of software modules – billing, inventory, customer management, marketing & production workflow.

✍ Wysetek Technologies [Apr 1992 – May 1993]: Software Programmer.

Development of software modules for billing, inventory, and customer management.

7. Personal Information

Nationality: Indian.
Languages Known: English and Hindi.
Qualification: Bachelor of Science (1989)
Current Location: Dubai.