Know our Trainer

Dr. Lalit Gupta

Foremost Cyber Resilience Expert across Asia Pacific, Middle East, and Africa regions

Profile Synopsis:

✓ Technically sophisticated and business savvy versatile leader, articulated communicator, ISO expert and SME in the domains of Information Security, Cyber Security, Risk Management and Business Continuity / Disaster Recovery, Privacy, and Pandemic Planning.

✓ 25+ years of work Experience in Delivering Business Value and Optimal Solutions in High-growth corporate Environments across all Business Sectors and Verticals like Govt. undertakings, BFSI (Banking, Finance & Insurance), IT / ITES, Pharmaceutical, Aviation, Manufacturing and Energy & Telecom.

✓ Hands-on SME being an individual contributor in all stages of Information Security Strategy, Governance and Management especially for defining the information security strategic roadmap by interfacing with core business functions and technology teams to identify required future state security capabilities, working with internal information security teams to secure the threat landscape, considering strategic risk areas of the organization.

✓ Adviser & Trainer to UAE Federal Govt. teams and Indian Defense Teams

Academic Credentials:

- ✓ **PhD** (Information Security) from USA
- ✓ **PhD Research Thesis Title** – The Analysis of How to manage Human Mind when Cultural shift happens after an Information Security Risk Assessment Exercise. Case Study – A SME Financial Sector Company in the Middle East.
- ✓ **MBA** (e-Business) from Canada
- ✓ **MBA Thesis Title** – A Study of Global e-Business acumen in comparison to e-Business situation in India

Professional Accreditations:

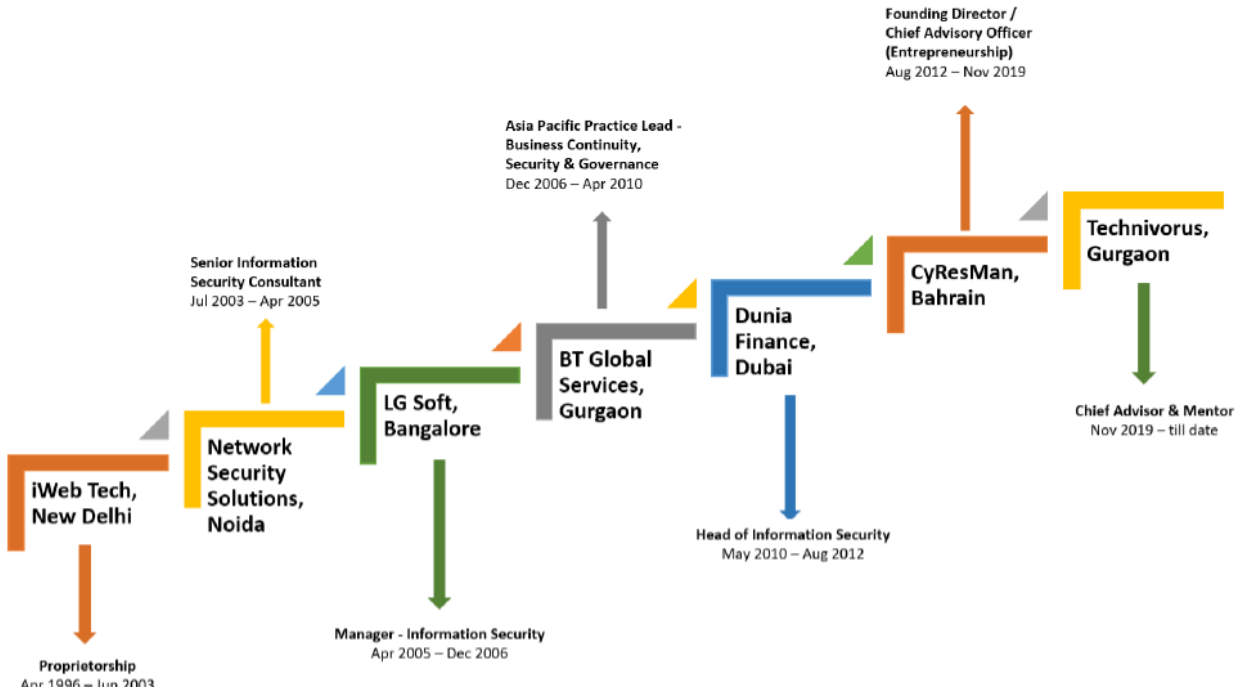
- **CISSP** (Certified Information Systems Security Professional), ISC2, USA
- **Lead Auditor** (ISMS, BCMS, SMS), RABQSA, Australia
- **Lead Auditor** (QMS, Asset Management), BeingCert, USA
- **CPD** (Certified Project Director) from GAQM, UK
- **CISA** (Certified Information Systems Auditor), ISACA, USA
- **GRCP** (Governance, Risk & Governance Professional), OECG, USA
- **CDPO** (Certified Data Protection Officer), BeingCert, USA
- **CPISI** (Certified Payment Card Industry Security Implementer, SISA, India
- **C-CISO** (Certified Chief Information Security Officer), EC Council, USA
- **CRISC** (Certified in Risk and Information Systems Control), ISACA, USA
- **ITIL v3** Foundation Examination qualified, Axelos, UK
- **CISM** (Certified Information Security Manager), ISACA, USA
- **BCCE** (Business Continuity Certified Expert), BCMI, Singapore
- **CHFI** (Computer Hacking and Forensics Investigator), EC Council, USA
- **MBCI** (The Member of Business Continuity Institute), BCI, UK
- **CCIO** (Cyber Crime Intervention Officer)
- **CCC** (Certified Cyber Criminologist)

Munirka, New Delhi – 110067 (India) +91 88025 05619 | +91 82875 09289 info@alvinintegrated.com
www.alvinintegrated.com

ALVIN INTEGRATED SERVICES

Know our Trainer

Experience Contour:



Career Snapshot:

- Being overall SME for Information Security and Cyber Security
- Providing the direction for data and cybersecurity protection and overseeing Technology Governance and Policies.
- Developing security strategy, security awareness programs, security architecture, and security incident response.
- Providing strategic risk guidance for IT projects, including evaluation and recommendation of technical controls.
- Reviewing and modifying Crisis Management Plan, Conducting Crisis Communications training for Crisis Management team in a simulated way
- Integration of ICAO Cyber Security framework with ISO 27001 for major Aviation players in the Middle East and Civil Aviation Authority in India.
- Conducting safety & reliability assessment on LNG (Liquefied Natural Gas) trains (liquefaction and purification facility)
- NESA (National Electronic Security Authority,) CIIP (Critical Information Infrastructure Protection Policy), and the IAS (Information Assurance Standards) implementation, review, and compliance handhold
- Collaborating with IT and compliance team(s) as needed and coordinates the IT component of both internal and external audits, federal and state reviews to ensure security programs are following relevant laws, regulations, and policies.
- Evaluating new cybersecurity threats and IT trends and develops effective security controls.
- Developing and overseeing effective disaster recovery policies and standards to align with company business continuity management program goals.
- Coordinating the development of implementation plans and procedures to ensure business critical services are recovered in the event of disasters or other incidents, and providing direction, support, and in-house consulting in these areas.

- Reviewing and monitoring the submission of accurate and complete Privacy Impact Assessments (PIAs) by the relevant business and support units within communicated deadlines based on the Operational Risk Management Calendar.
- Assisting in cultivating awareness on privacy and data protection by developing and conducting training sessions, awareness campaigns and breach reporting drills
- Building a strategic and comprehensive privacy program that defines, developed, maintained, and implemented policies and processes that enabled consistent, effective privacy practices which minimized risk and ensured the confidentiality of protected information, paper and/or electronic, across all media types. Ensured privacy forms, policies, standards, and procedures are UpToDate
- Performing / overseeing initial and periodic information privacy risk assessment/analysis, mitigation, and remediation.
- Conducting related ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions.
- ISO 22301 & ISO 27001 implementation leading to integrated certification
- Driving Top Management Crisis Simulation Exercise with multiple scenarios like Cyber Attack, Fire, and loss of key people due to Pandemic attack, Central Bank Regulations implementation pre-audit assessment
- Understanding and interacting with cross functional disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems, and services
- Assisting with the overall business technology planning, providing a current knowledge and future vision of technology and systems
- Risk review on holistic level for the Central Risk team, Supervising VAPT exercise conducted by external vendor.
- Conducting Disaster Recovery and Cyber Security Risk review on Command & Control setup including SCADA and ICS Security
- SOC team technical training on incident handling and Management, Top Management Crisis Simulation Exercise
- Managing the SOC Services as CSM (Customer Service manager), conducting risk reviews with Senior IT management team of and recommending proactive controls. Risk Reviews of existing Incidence management Infrastructure.
- Conducting Risk Review of online Education and Exam infrastructure leading to a fraud identification. conducted forensics and investigation leading to conviction of fraudsters
- Leading a team of Security Experts for architecting & delivering Security Solutions for Enterprises.
- Instrumental in providing Consultancy and delivering solutions on Information Security propositions including MSS (Managed Security Services), and IDM (Identity Management), specializing in ORM (Operational Risk Management) and BCM (Business Continuity Management) for clients in Asia-Pacific region.
- Preparing and issuing Advisories and Incident and Vulnerability notes based on global attack patterns
- Acting as Virtual Country Security Manager / Business Continuity in Country Lead, responsible for supporting the Chief Security Officer (CSO), and Country Management Team with the primary role of being the Single Point of Contact for all BCM related questions/issues and Incident Management
- Defining requirements for security-related technologies such as intrusion detection systems, authentication systems and access control, network vulnerability, Anti-Virus, and various other countermeasures in accordance with ISM standards.
- Creation of BCP & DR, pre-sales, technical presentations, technical papers on latest security best practices and emerging trends in vulnerabilities & attack patterns, conduct security evaluation on client networks, draft information security policies & standard operating procedures, conduct training on various security related topics.