DATTATRAY BHAT **Mobile:** 09323310491 ✳ **E-Mail:** d_p_bhat@yahoo.com

SENIOR IT PROFESSIONAL: Information Security Operations & Compliance

CAREER SNAPSHOT

- **Over 14 years** in driving overall IT Security Operations inclusive of defining the IT roadmap, budgeting, technology evaluation with diverse work experience of **IT & Information Security**.
- A keen planner, strategist & implementer with demonstrated abilities managing entire **IT security operations**.
- Proven record of directing corporate IT initiatives while participating in planning, root cause analysis and implementation of information security solutions.
- Expertise in leading **Security Operations** encompassing **User ID Management, Security Health Checks of Servers & Network Devices, Patch Management, Vulnerability Assessment, Application Security etc.**
- Deft at handling **multi-vendor networks** with a variety of operating systems and security products.
- Abilities in ensuring a **secure, reliable, and centralized IT environment** that will help better balance organization's needs for security and functionality.
- An effective communicator with excellent interpersonal skills and strong analytical, problem solving & organizational abilities.

SKILL SET

- Strategy & Tactical Planning	- Project Management	- Network Security Management
- Information Security	- Application Security Testing	- Troubleshooting
- SOX Compliance	- Data Migrations	- Resource Optimization
- Technological Enhancements	- Risk Mitigation & Control	- ISO27001 Implementation
- Security Assessments	- Audits & Compliances	- Vulnerability Analysis
- PCI DSS Implementation		

IT Security & Compliance:
- Analysing as well as reviewing the physical & logical security measures and safeguarding the information resources of the enterprise.
- Formulating the information security policies & information security guidelines and ensuring adherence to compliance related to IT Security policies.
- Conducting risk assessment, vulnerability assessments, penetration-tests and coordinating IT Security framework design and implementation.

Operations:
- Administering, implementing & maintaining security through a methodical approach /security tools and conducting GAP analysis and risk assessment procedures.
- Assessing organisational requirements for security & implementing security software systems against various attacks and executing back-up strategy, ensuring scheduled / unscheduled backups.
- Managing customer service operations for rendering and achieving quality services.

Domain Expertise: Automobiles, Telecom, Aviation, Financial Services, Media, Government and IT Services.

ORGANISATIONAL SCAN

Since Apr'08: International Business Machines (IBM), Pune as Security Advisory Specialist

Accountabilities
- Spearheading **security operations** encompassing SAS70 / SSAE16 Testing, AUP Testing, User-ID Management, Security Health Checks, Patch Management, VA/ PT, AV Management, Management of various security tools like Websense, ISA, RSA Secure-Id, etc.
- Pivotal in reviewing architecture & design and securing coding assistance to Developers in fixing application compliance issue in accordance with PCI DSS and SOX compliance.
- Regularly suggesting methods to improvise processes to assure compliance with organization security policy and industry best practices.

Highlights:

- Successfully established the Security Operation Centre & implemented RSA Envision for one of the leading Telecom Service Provider.
- Performing as Service Line Owner for India / South Asia Accounts.
- Extensively worked on AppSec of Telecom Enterprise products & design architecture.
- Recognised for developing application security testing framework in a customer account.
- Built AppSec Team which received many appreciations from customer.

Jan'06-Apr'08: Kale Consultants Limited, Pune as Senior Manager – Information Security

Accountabilities

- Deftly handled the migration of BS7799 Certificate to ISO 27001 in Jun'06.
- Acted as IT Lead for Knowledge Process Outsourcing Centre and responsibly handled the IT Operations.
- Pivotal in managing PCI DSS Certification for Managed Processes Centre.
- Executed Internal Audits and ensured compliance to security policies.
- Instrumental in maximizing network availability & connectivity by expert troubleshooting.
- Handled configuring & management of firewalls, routers & switches.
- Carried out Vulnerability/Threat Analysis & drafted Security Assessments & Status Reports related to IT Security.
- Analysed Security Analysis Reports for security vulnerabilities and investigated complex information security issues.

Feb'04-Dec'05: Apara Enterprise Solutions Pvt. Ltd., Mumbai as Technical Leader – Security Services

Accountabilities

- Successfully implemented Security Solutions for customers.
- Rendered Post-sales Support for Security Solutions and implemented AntiSpam Solution.
- Conducted Vulnerability Assessment & Penetration Testing for customers.

Jan'00-Feb'04: **AFL Pvt. Ltd., Mumbai as Senior Executive – Web Services**

Accountabilities

- Pivotal in implementing:
  - Antivirus & AntiSpam Solution.
  - OSPF Routing Protocol in AFL WAN.
  - Checkpoint Based Architecture.
- Managed the BS7799 Information Security Certification.

KNOWLEDGE PURVIEW

- **Application Testing/ Auditing:**
  - *Types of tools:* Vulnerability Scanners, Fuzzers, Web Proxy Editors, Decompilers, Memory Viewers, Password Crackers, Browser Extensions, Spiders, File/Registry Monitors, API Viewers.
  - *Some Tools:* IBM Rational (Watchfire) AppScan, HP (SPI Dynamics) WebInspect, Paros Proxy, Acunetix Web Application Scanner, Tamper IE Tool, Wikto, Nikto, WebScarab, NStalker, Nessus, etc.
  - *Methodology:* A hybrid methodology that consists of the OWASP, OSTMM, NIST and Industry Best Standards will be involved to test the application. A combination of rigorous manual testing and automated tools.
- **Remote Access & Managed Security**
  - *Remote Access*
    - RADIUS, 2-Factor Authentication, Dial-Up Networking, VPN, Single Sign-On, Certificate Based Authentication, Remote Access Servers, Terminal Servers, Remote Control Programs, SSH, Desktop Security.
    - Products: RADIUS, Kerberos, i2 Security, LDAP.
  - *Managed Security Services*
    - Monitoring security components in a Network for e.g., Firewalls, Routers, NIDS, CMS, HIDS, Antivirus etc.
    - Products: Qualysguard, RSA envision and Guardium for DBs.
- **Forensics, Research and Penetration Testing**
  - *Forensics Investigation and Research*
    - Log Audit & Analysis, System Forensics, Incident Handling, Chain of Custody Issues, md5 Signatures, Log Correlation, Investigation, etc.
    - Products: Stellar, md5, Net Forensics, Encase, Filemon, TDImon, Regshot, IDAPRO, OLLY Dbg.
  - *Penetration Testing (Ethical Hacking)*
    - Information gathering and reconnaissance, identifying vulnerabilities and target selection, port and Firewall Scanning, OS Fingerprinting, DNS, SMTP, denial of service, exploiting vulnerabilities & privilege escalations and covering tracks
    - Products: Metasploit, Core impact.
    - Manual Testing and searching security sites.

- **Perimeter Security**
  - *Intrusion Detection & Prevention*
    - Network Intrusion Systems, Host Based Intrusion Systems, Policy Enforcement Systems, Proactive Scanning, Integration Issues, Signature Design, etc.
    - Establishing and performing operations of Security Operations Centre (both in-house and subcontracted).
    - Products: Snort, iPolicy IPF, Imperva and F5 WAFs.
  - *Security and Network Engineering*
    - Security Design, Network Design, Capacity Planning, Protocol Analysis, Security Systems Integration, Network Routing, Network Redundancy, Layer 3 Switching, Policy & Role Based Authentication, Firewalls, Routers, VPN.
    - Products: Checkpoint, Nokia IPSO/ SMARTSPLAT, Cisco & Foundry Routers and Switches, Cisco PIX, IPtables, Tomahawk, Intruder Pro, Karalon.
- **IT Service Management and ISMS Integration**
  - *ITIL and ISMS*
    - ITSM support and release implementation experience to contribute toward the success of customer technology initiatives.
    - Availability, Change, Incident, Problem Management & Coordination.
    - Supports new and ongoing ITIL initiatives and their integration.
    - Coordinates activities with all service providers to deliver end-to-end services to the business.
    - Provides support for implementation issues and questions. Supports development and deployment of new processes and/or enhancements to existing processes
  - *ISMS*
    - Preparation, implementation and continuous improvement of policies, procedures and forms.
    - Reviews documentation and technical specifications of any processes under deployment or consideration.
- **Security Management Services & IT GRC**
  - *Vulnerability/Risk Analysis*
    - Security Policy Design and Business Continuity Planning, Vulnerability and Risk Assessment, Trust and Threat Modelling, Security Auditing.
    - Products: ISS Internet Scanner, Qualys, Nessus, Outworks from Outscan, Retina, LanGaurd, Saint.
  - *IT GRC and ISMS Audits*
    - Security Audits & compliance to security in accordance to ISO 27001.
    - Worked on RSA Archer EGRC tool.

SCHOLASTICS

1998 **B.E. (Electronics)** from V.P.P.C.O.E, Sion, Chunabhatti, University of Mumbai.

Certifications:

- Certified Information Security Manager (CISM)
- Project Management Professional (PMP)
- IBM Certified IT Specialist
- ISMS Auditor/ ISO 27001: 2005 Lead Auditor
- Certified Ethical Hacker (CEH)

PERSONAL DOSSIER

Date of Birth:	9th November 1974
Linguistic Abilities:	English, Hindi, Marathi and Kannada
Address:	B 503 Mayur Panorama CTS No 6611 Nehru Nagar Pimpri, Pune: 411018

~ Please refer to the annexure for critical projects ~

~ ANNEXURE ~

Project: **Compliance Posture Improvement**

Brief: Handled all the Project Management responsibilities of SAS70 deliverable. Controlled customer environment and developed strong Governance Mechanism. Pivotal in managing primary / secondary controls to assess the adherence to documented processes. Following were the expected benefits from the above controls:

- Timely escalations to Project DPE, Tower Leads.
- Proactive step to ensure adherence to agreed Process and Procedures.
- No Observations / Issues in Reviews / Audits.
- Help Maintaining / sustain the compliance level for the Account / Project.

Solution: Enhanced the Compliance Posture for the account, following solution / action were implemented. Executed proactive 100 % Compliance Testing to prevent noncompliance & remediation of any issues identified.

- User ID Management
- Change Management and Problem Management
- Security Health Check
- Issue Management
- Daily Metrics reporting to Account & IMT Leadership Team
- Education / Awareness Session to the Operation Team on the Processes and tools to improve the Operations efficiency and compliance posture by the Security and Risk Assessment Team.
- Awareness Sessions were carried out on the SAS 70 Control Objectives and Control Activities.
- Education Session carried out on Agreed Upon Procedures (AUP)

Role: Worked as a **Project Manager** and performed the following duties:

- Coordination with Process Owners & Compliance Team Members
- IBM Account Management
- Update Stakeholders with status on the Compliance Testing on daily basis,
- Timely Escalation to Tower Leaders, DPE and IBM Senior Management,
- Coordination with External Auditors - PwC and Internal Auditors - Compliance & Regulator Team
- Timely Responses to Data Requests from External Auditors during Final Testing
- Successfully completed following tasks as part of this Project,
    - Rationalized Risk and Control Framework
    - Mapping Policies and requirements to the business
    - Standardizing Risk and Compliance Processes
    - Aggregated Data for Monitoring and reporting

Project Results

- **Client Satisfaction:** As customer is listed in New York Stock Exchange, SOX Compliance is one of the regulatory requirements. SAS70 / AUP report being requirement for SOX Compliance for outsourced clients, producing Positive Report for SAS70 / AUP testing satisfied the client on IBM Deliverables and also ensured adherence to agreed processes through Third Party Testing.
- **Quality of Deliverables:** Implementing above controls and following IBM Global Processes ensured Quality of deliverables to Customer.
- **Performance of the IBM Team:** Awareness on agreed IBM Global Processes to IBM Team helped to perform with Global IBM guidelines and deliver as per requirements.

Project: **PCI - DSS Compliance**

Brief: Kale Consultants Limited (my previous organization) is a leading solutions provider to the global Airline, Airports, Logistics and Travel (AALT) industry. Committed to innovation and excellence, Kale delivers world-class software products, technology, managed process, hosting and consulting services. Kale employs over 1600 talented professionals who focus on delivering quality service to over 120 satisfied customers across 5 continents. As part of the offerings to customers / clients, new requirement of handling Credit Card Data was requested by one of the customer. This requirement demanded for new compliance / regulatory requirement for Kale Consultants Limited of being compliant for Payment Card Industry Data Security Standards (PCI-DSS). Looking at the new Business opportunity, Kale's Senior Management decided to go head with investing in PCI-DSS compliance certification.

Role: Worked as a **Project Manager**, following were key decisions made by me,

- Control Case Vendor been finalized for the PCI-DSS testing and certification, other vendors were not supporting from Pune Location, not prior experience on PCI-DSS, costing was high.
- Coverage of both Primary and DR site Implementation of new controls made additional efforts to be put in by employees, additional efforts were found to be difficult to be implemented. Following action were taken to overcome them,
- Training and Education Session to employees having access to Credit Card Data on Payment Card Industry Data Security Standard
- Implementing the controls using top down approach.

Solution Payment Card Industry Data Security Standard (PCI-DSS) being very new to Kale and Indian Industry, delivering the certification was difficult. Following were my responsibilities, specific tasks

taken by me to ensure Kale being PCI-DSS Compliant and help Kale to get new Business opportunity.

- Identified the Vendors authorized to certify PCI-DSS Compliance in India
- Mapped the PCI-DSS Controls with currently implemented controls
- Analysis done for non-implemented controls on Cost Involvement, Implementation Feasibility, Training
- Calculation for total cost of ownership for the Project

Project Results

- **Client Satisfaction:** As per customer / client requirement, Kale could implement the PCI-DSS requirement for handling the Credit Card Data owned by Customer. Kale getting PCI-DSS certification made customer to have good relations with Kale and confidence in handing over critical data for Processing as part of Business Processing Outsourcing. This also ensured adherence to agreed processes through Third Party Testing i.e. Control Case testing for PCI - DSS controls and giving independent review results for implemented controls for maintaining Information Security.
- **Quality of Deliverable:** Implementing PCI-DSS controls ensured Quality of deliverables to Customer by following Best Practice in Handling Credit Card Data.