Amit Kumar Verma

Global Information Security Manager
ISG Novasoft Technology, Bangalore
Mobile: +91 9986502867 | Email: amit0869@gmail.com

Objective: Leadership role in Information Security and Global Risk Compliance.

"High energy Information Security, Operation Risk & BCP professional having 12+ years of experience in running effective corporate security program spanning expertise in IS & GRC design, roll out, monitoring, improving in global companies. Aspiring for challenging leadership roles to deliver operational excellence by leveraging on my knowledge, expertise & skills."

Executive Summary

Experienced in designing and delivering effective Corporate, Information Security and Business Continuity program

- Drive organization-level corporate, information security & business continuity function, develop & enforce policies, processes and best practices to achieve security compliance and maintain optimum BCP & security posture throughout.
- Make high-stakes decisions, handle complex security issues, provide expert advisory inputs and manage critical security projects.
- Design, implement & enforce effective information security & business continuity programs.

Profile Summary:

Prior Experience: 12 years of progressive Information Security, Business Continuity, Corporate Security Management, Audit & Customer Service experience with top MNCs across BFSI, IT & ITES, ISP, Media & Entertainment verticals.
9 years of managerial experience working with C-level executives (including functional reporting to CEOs) drawn from cross-functional domains.
Education:
MBA (Marketing, ISO 27001:2005 Lead Auditor, CEH & Hardware and Networking Diploma).
Occasional contributor on Security topics and Guest Speaker at Security Conferences & Training Programs.

Areas of Expertise: Specialize in setting up Information & Corporate Security/BCP function from ground up in MNCs

Information Security & Business Continuity Management

- Information Security Governance, Risk & Compliance (GRC)
- Developing & enforcing of Information Security Policy & Practices
- GRC program for ISO 27001:2013 ISMS, PCI-DSS, SOX, GLBA, FFIEC, CDSA, Basel III, CNIL, ISO 22301 BCM Standards
- Enterprise Risk Management - Assessment and Mitigation
- Security Program monitoring and improving through Security Metrics
- Identity and Access Management (IAM) Solutioning & Administration
- Security Awareness, BCP & Crisis Mgmt. Training, Design & Promotion
- Security Incident Management
- Tracking, Reporting & Resolution
- BCP- BIA, Planning, Documenting, Implementing, Training, Testing
- Pandemic Planning- H1N1 Monitoring, Preventive Measures & Advisory
- Conduct Operational Risk Management and Governance.

Corporate Security

- Physical Security Controls Rollout & Review
- Manpower planning, hiring & training
- Access Control, CCTV & Fire Safety
- Evacuation Drills, ERT & Travel Security
- Environment, Health and Safety (EHS)
- Labour Law Compliance

Executive Oversight

- Vision, Strategy & Execution
- Budgeting & Cost Control
- Program & Project Management
- Team Building, Mentoring & Leadership
- Stakeholder Management
- Management Reporting & Updates

Soft Skills Competencies:

- Strong Communication Skills and adept in building & presenting Business Cases, highlighting open risks & vulnerabilities with relevant solutions to Management
- Proven interpersonal skills- team player/builder, superior documentation and training skills.
- Ability to stand by my convictions when it comes to matters of security, business ethics & personal integrity.
- At ease in high stress, fast-paced environments with multiple responsibilities & meet aggressive deadlines.
- Ability to connect, liaison and engage with all levels of management & employees and bring about mind-set change.

- Effective trainer with ability to translate technical concepts to lay audiences.
- Work as part of geographically-dispersed team with minimal supervision and deliver results.
- Plan and coordinate multiple projects simultaneously - multi-tasking capabilities.

Professional Work Experience:

- November 2014 – Present ISG Novasoft Technology ITPL, Bangalore

Manager-Information Security
Reporting to: Director – Information Security

Principal role in driving information security function at ISGN India and US

- Recruited to prep and roll out ISO 27001 ISMS across ISGN and be responsible to deliver the Group's Information Security Program at organizational level across 8 Business Lines covering 1000+ users across 3 locations.
- Risk Management, Security Program Management, Data Security, Policy Creation and Maintenance, Regulatory
- Conduct Operational Risk Management and Governance.
- Compliance, Standard Compliance, Security Project Management, Incident Management, Network Security, Business Continuity/Disaster Recovery, Security Architecture.
- Exposure to deployment of Security and Governance related Project Management.
- Key role in improving company's information security strategy, practices & effecting enterprise-wide culture change.
- Maintaining Security Compliance Framework as per SG Security policy & directives.

Key Achievements:

- Revamped Identity and Access Management Governance framework (Sail Point) and rolled out enterprise-wide
- Implemented enhanced security controls project to secure sensitive data and improved policy exception process
- Improved process rigor for data leakage protection (DLP) for outbound emails using Symantec DLP
- Developed control framework for security health checks monitoring in BAU mode
- Conduct Operational Risk Management and Governance.
- Raised visibility of information security function company-wide through Risk Culture program and revitalized Security Awareness
  Program – New Joiner Induction, Risk Newsletter, End-user Communication, Participation in Events, etc.
- Revise end user documentation - Security Policies, Procedures, Cheat sheets, Flyers & Awareness Presentations
- Streamlined Risk Assessment Program for critical IT projects, sensitive applications and outsourced vendors
- Performed gap analysis for ISMS implementation and prepared business case for roll out
- Ran periodic User Access Review campaigns (applications, infrastructure, mailbox access) and ensured 100% compliance
- Audit interface and responsible for closure of audit recommendations and non-conformances within agreed deadlines
- Implemented Change Management system with change verification and Coordinated and validate periodic 3rd party vulnerability and penetration testing
- Work with sales team on pre-sales and post-sales customer security evaluations and Facilitated SSAE 16 SOC 2 security audit.
- Perform control mapping from GLBA, ISO27000 and Perform company-wide risk assessment
- Developed company-wide Risk Register and Identify potential risk, consult on correcting or reducing risk, report if uncorrected
- Assist in the development of a risk register and Perform Vulnerability assessments on projects and Penetration Testing on projects or existing infrastructure.
- Perform vendor security assessments and Risk assessments on new projects, identify and reduce risk &Consult with Security Operations Team on security events

U.S. based ISGN (http://www.isgn.com) is a leading full service provider of mortgage technology and services, impacting over 5.5 million of mortgage customer.

- March 2013 – August 2014 Theorem India Sanjay Nagar, Bangalore

Manager – Information Security (Role equivalent to Head of Security, India)
Reported to: Country Head Theorem India, dotted line reporting to Direct CTO-- Worldwide Content Protection and Anti-Piracy
Maintaining Security Compliance Framework as per Theorem Security Policy.

Key Achievements: **Received Spot Award for IS Governance Initiatives**
Achieved: **Industry's leading digital security standard CDSA certification**

- Built Theorem India's Information Security and Corporate Security Program from ground up to global standards fully aligned with the Group's Security Policy.
- Set up Country Security Council for Theorem India to serve as steering committee for security function SPOC for Security function and offer expert advisory to Management on security matters
- Established Security Governance, Operational Risk & Compliance (GRC) program for Theorem India
- Handled Internal & Statutory Audits for IS including SOX compliance requirements – UL Management auditors
- Provided guidance & handholding for CDSA & MPAA compliance to onsite locations.
- Drafted and implemented site-specific security policies, procedures & best practices
- Instrumental in raising visibility of security function across BUs – security handbook, induction & awareness programs
- Enhanced Environment, Safety & Health (EHS) Program by improving safety posture – equipment & staff training
- Lead and successfully coordinated (5 instances, <12 mins) site Evacuation Drills (planned & unplanned)
- Managed crisis situations (general shutdowns, cab strikes) with advisory to management on office open/shut decisions

Theorem is the world leading provider of delivering digital solutions that create value and connect brands with audiences. Specialized expertise across the digital marketing and advertising technology landscape leveraged to help you design, develop, manage, and/or integrate platforms.
This class will focus on the areas of data privacy and data security, potentially the biggest "data" issues that marketing communications professionals will face over the course of their careers. As such, the class will address the rapid move of companies toward digital marketing efforts, and the coming world of connected devices in the Internet of Things.

- July 2010 – March 2013 Concentrix Technologies Bangalore, Chennai

Asst. Manager – Information Security (Role equivalent to Head of Security, India)
Reported to: Head-IT, dotted line reporting to Concentrix India Country Head - Principal role in driving information security function at SG GSC India. Maintaining Security Compliance and PCI- DSS Framework as per Concentrix Information Security and Business Requirement.

- Proving company's information security strategy, practices & effecting enterprise-wide culture change.
- Maintaining Security Compliance Framework as per SG Security policy & directives.
- Revamped Identity and Access Management Governance framework and rolled out enterprise-wide.
- Implemented enhanced security controls project to secure sensitive data and improved policy exception process
- Improved process rigor for data leakage protection (DLP) for outbound emails using Symantec DLP
- Developed control framework for security health checks monitoring in BAU mode
- Raised visibility of information security function company-wide through Risk Culture program and revitalized Security Awareness
  Program – New Joiner Induction, Risk Newsletter, End-user Communication, Participation in Events, etc.
- Revise end user documentation - Security Policies, Procedures, Cheat sheets, Flyers & Awareness Presentations
- Streamlined Risk Assessment Program for critical IT projects, sensitive applications and outsourced vendors
- Performed gap analysis for ISMS implementation and prepared business case for roll out
- Ran periodic User Access Review campaigns (applications, infrastructure, mailbox access) and ensured 100% compliance

- Audit interface and responsible for closure of audit recommendations and non-conformances within agreed deadlines
- SPOC for Security function and offer expert advisory to Management on security matters.
- Established Security Governance, Risk & Compliance (GRC) program for Concentrix India.
- Handled Internal & Statutory Audits for IS including SOX compliance requirements.
- Provided guidance & handholding for GLBA, SSAE16, PCI-DSS compliance to onsite locations
- Drafted and implemented site-specific security policies, procedures & best practices
- Instrumental in raising visibility of security function across Bus – security handbook, induction & awareness programs

- October 2009 – May 2010 Paladion Networks Bangalore, Chennai

Manager – Information Security SOC (Role equivalent to Head of Security, India)

Reported to: AVP SOC, Maintaining Security Compliance and PCI- DSS Framework as per Paladion Security Operation ODC - Information Security and Business Requirement.

Key role in aligning Information Security Program with global policy and developing BCM Program company-wide

- Recruited to form Security Office at Paladion Networks and be responsible to deliver Information Security &Business Continuity Program at organizational level for Bangalore ODC in line with corporate security policy.
- Member of core security team set up to provide strategic direction to Information Security & Business Continuity functionfully aligned to ISO 27001:2005 ISMS.
- Pivotal role in optimizing company's security strategy, practices & effecting company-wide culture change.
- Designed and enhanced security program controls mapped to ISO 27001 ISMS requirements
- Close liaison with related governance functions – Physical Security, Facilities, IT, HR, Legal to meet global security standards.
- Established BCM Life cycle (covering BIA, deptl BCPs, Implementing, Training, Testing, Improvement, Maintenance)
- BCP Documentation: Developed BIA format & departmental BCP documents for critical business functions

Audit Prep Work Program Management:

- Coordinating & participating in revision of Security Policies, Procedures & Practices with policy owners
- Collating required evidences and preparing documentation - creating binders for policies & procedures, audit evidences &records for auditor reference. Prep work management with periodic reminders and regular updates to Capgemini leadership.
- Organizational preparedness – training, briefing key stakeholders, enterprise-wide email communication, etc.

Established & implemented a comprehensive Security Awareness Program:

- Conducted role-based Security Awareness Training Program (3 annual cycles) for Paladion Networks Bangalore staffers (around 300persons) in about 16weeks time scheduled alternate days. Followed up to ensure 100% training coverage.
- Designed & Developed Presentations, Security Best Practices Pamphlets, Security Awareness Posters & Wallet Cards.
- Launched monthly security newsletter "Capgemini Infosec News" and served as Editor – write, collate articles, design, layout & e-publish

August 2006 – July 2009 Capgemini, India Bangalore, Chennai

Lead – Information Security -GM (Role equivalent to Lead Security, India)

Reported to: Snr Manager, Information Security and Compliance, Capgemini Corporate Information Security and Business Requirement.

Key role in aligning Information Security Program with global policy and developing BCM Program company-wide

- Designed and enhanced security program controls mapped to ISO 27001 ISMS requirements
- BCP Documentation: Developed BIA format & departmental BCP documents for critical business functions
- Driving & project management of preparation work at Capgemini India office for annual PCI-DSS Level 1 Service Provider
  Assessment by Verisign, Inc.
- Designed and enhanced security program controls mapped to ISO 27001 ISMS requirements
- Close liaison with related governance functions – Physical Security, Facilities, IT, HR, Legal to meet global security

standards.

- Established BCM Life cycle (covering BIA, deptl BCPs, Implementing, Training, Testing, Improvement, Maintenance)
- BCP Documentation: Developed BIA format & departmental BCP documents for critical business functions.
- Conducted Business Impact Analysis (BIA) by coordinating with departmental heads in both US & India.
- Coordinated conduct of 3 BCP Functional Remote Access Tests and Table Top Exercises at BLR & US offices (includes planning, Coordinating with IT & Ops teams, employee communications, post-test data gathering & reporting)

- Jan 2005 – Jul 2006 Progeon, Infosys BPO India Bangalore

Information Security-Senior Associate (Role equivalent to Lead Security, India)
Reported to: Senior Manager-Information Security
Signed up to spearhead the setting up of Data Security as a distinct IT Security service vertical for Client Security Services. Responsible for running the division as a profit centre in tandem with other IT Security SBUs.

Key Roles & Responsibilities:

- Member of core security team set up to provide strategic direction to Information Security & Business Continuity Functionfully aligned to ISO 27001:2005 ISMS.
- Participate in management meetings for business strategy & direction.
- Prepare/Approve Request for Proposals (RFPs) & quotations for clients.
- Coordinate conduct of audits & follow up on closure of NCs found during audits & assessments.
- Build and sustain client relationships, support pre-sales activities for key clients.
- Close liaison with related governance functions – Physical Security, Facilities, IT, HR, Legal to meet global security standards.

Education

Year	Degree	University
2002-2004	PGDBM	Master School Of Management
1999-2002	Graduation (B.A. Economics)	Shia Degree College-Lucknow University
1999	High Secondary (Plus Two)	CBSE Senior Secondary School-NOS
1996	High School (10th)	Lucknow Public School

IT Certifications and Trainings

- BS ISO/ IEC 27001:2005 Information Security Management System Lead Auditor
- Six Sigma Black Belt Certification (ASQ) (Skill Global Institute)
- MCP Certification
- Hardware and Networking
- ISO9001 Trained Certified
- ISO 27001 LA and ISO 9001 trained Certified
- PCI DSS Implementer
- CEH Trained
- Six Sigma Black Belt Trained Certified
- GLBA compliance
- SSAE16 compliance audit

PERSONAL PROFILE

Date of Birth:	20th July, 1980
Marital Status:	Married
Languages known:	English, Hindi