Vivek Srivastava
Cell No-xxx-xxx-xxxx
Email: xxxxxx.xxx@xxxxx.xxx
Los Angeles CA-USA
https://www.linkedin.com/in/vivek-srivastava-70743915/

Governance Risk Compliance/Cyber Info Security/Risk Advisory/Forensic/Threat/Incident & Vulnerability Management/Archer GRC Developer

PROFESSIONAL SUMMARY:

- 13 Years Exp in Cyber Information Security-GRC RiskVision,Archer Implementation & Secure System Development
- NIST Risk Management Framework (RMF), 800-171, 800-53,CIS Critical Security Controls,GDPR,GLBA,
- FFIEC Examination, Malware techniques, defenses, Forensic Analysis, Secure Web Proxy,FDIC exams, System Hardening Benchmarks, Secure e-mail Gateway,ISO 27001 ISMS,FIPS 199,FIPS 200, SWIFT Customer Security
- Expertise with GRC Tool Archer,Agiliance, Business Analysis, High Level Design, Source Code
- Cyber Forensic Analysis Tool Encase, Access Data, FTK, DEFT, HXD,CAINE,File Signature,Registry Analysis
- Execution of Project Plan, Budgeting, Cost Management, Scheduling Plan, Metrics Report
- Compliance Manager, Policy Manager, Enterprise Risk Management, Vendor Risk Management
- Threat & Vulnerability Management, Incident Management, Automated Data Collection, Security Assessment. Audit Management, Business Continuity Management, Workflows
- Information Security Risk Management based on BITS Framework, COBIT, NIST 800-30,NIST 800-53, ISO 27001:27013, , ISO 27002, , ISO 27003,CIS CSC, PCI DSS,Compliance Wireless LAN,NERC Controls
- RSA Archer e-GRC Platform Version 5.5 (Application Builder, Access Controls, and Data Feed Manager, Business Continuity Management, Audit Management, Administration-Reports).
- Experience in LDAP, Simple Network Management Protocol, Authentication, Single Sign-On
- Experience in Risk Management,Vulnerability Assessments, Authentication & Access Controls, Splunk Version 6.6.1 Integration/Data Import Feed
- Hands on in IT-GRC Domain with Regulatory compliance such as PCI/SOX/HIPAA/NIST/Cobit, FISMA SP 800-18
- Experience in Firewalls, Intrusion Detection Systems, Network switches, routers, Network Designs, VPN, TCP/IP communications, Cloud Computing,Technical Control,Management Control,Operational Control,Privacy Control
- FileDisclosure, File inclusion, XSS, CRLF Injection, path Injection,SEL Injection, Weak .htaccess,Backup file disclosure
- Developed Test Scenario for Cluster/n-Tier Setup, Installation, Upgrade, Update, System, Integration
- Implemented Performance Scalability Test, Big Data, Estimation, Planning and Execution
- Developed Penetration Testing, Security Testing,Buffer Overflows,Burp Suite,Brute Force,OWSAP Top 10,SqlMap,Cenzic,WPScan
- MyOneLogin, Multi Factor, Cookies/Certificate based Web Application, SAML, Single Sign On.
- iKey/USB/OTP Token based Web Application, Smart Card/Public Key Infrastructure (PKI) based Web Application
- Scanning insecure server configurations, validating database injections with, JSP,ASP,SQL,XPath,PHP
- Banking Domain –Cryptography, SSL/HTTPS, Encryption-Decryption-Web Based Application.Financial Application,Legacy Systems
- Developed test scenarios for Web Based Browser Two Factors, ID Tool, Authentication Ladder.
- Developed test scenarios for Jasper Soft Reporting Tools to Manage the Report and Dashboard
- Experience in Team Management, Task Management, Task Tracking and Report Management.
- Experience in Agile-SCRUM Methodology Development and Release Process.
- Developed Set Up for Configuration Management [CVS/SVN],Cherwell,Microsoft Sharepoint File Management
- Experience in testing protocol such as HTTP, HTTPS, SMTP, POP3, IMAP4, SSL, FTP,VPN,Telnet
- Experience in Web Services Deployment, Web Security. API Testing. SQL Injection, Cross Site Scripting and Fiddler, Burp and Fortify Security Tools
- Experience in Web Performance Load Test Tools 4.2,Mobile-e-commerce J2MEE based Web Application
- UNIX, flavors (LINUX) and Windows platform and MYSQL5.5 for Apache,Tomcat,IIS Deployment
- Mobile/Windows/Desktop Application, Client/Server Application.
- Deployment of Web Based JAVA/J2EE /J2ME Application/VC++/MFC/C#/Dot Net Application.
- Experience in Installer using Install Shield X for VC++/MFC Application.

EXPERIENCE:

- Bank of The West-Cyber Security IT-Application Er, Assistant Vice President from April 2016-Till Date
- BNY Mellon: Information Security Analyst Vulnerability Manager-RSA Archer GRC, Oct 2015 – March 2016.
- Deloitte: Governance Risk Compliance RSA Archer SME, July 2015 - Sept 2015
- Infosys: Archer GRC Senior Engineer, April 2015 – May 2015
- HCL Technologies: GRC Archer Associate Consultant, Dec 2014 - March 2015
- RiskVision-Agiliance: Governance Risk Compliance Lead, March 2008 - Nov 2014.
- OutworX Corporation: Senior Software Engineer, April 2004 - Feb 2008

Educational Qualifications:

- **Master in Computer Application** from **School of Management Sciences, Varanasi-India**

Technical Experience Summary:

Security Scanner Tool	Web Inspect7.5, Nessus 3.0, Qualys, Arcsight, Appscan, SkyBox, n-Circle, Eye-Retina, NetIQ
Programming-Language	C++/Java and .Net, Ajax, Java Script, Groovy Script, WSDL/XML/SOAP/REST/JSON, SOAP UI, XMLSpy, UML modelling, DevOps, Jenkins, ODM, BAM,XQUERY,XPATH,XMLAJAX,XML-DTD,JSON
Web Technologies	Web 2.0, AJAX, Servlets, JSP, Applet, HTML, HTML5,DHTML, XML, Asp. Net,jQuery,Angular,Node.js,,Python/Powershell
C++ Technologies	Windows Programming (Win 32), STL, MFC, Microsoft VC++ Studio.
RDBMS	Oracle 11g, MySQL5.5, Aqua Data Studio 12.0, PostgreSQL 10
Web Server	Apache 2.0, Tomcat 5.0, IIS5.0, IIS6.0
Operating Systems	Windows 2000 Professional, XP Professional, Linux, MAC (Macintosh), FreeBSD (UNIX), Windows Vista/Windows 2003/Windows 2008 Server
Project Management Tool	Web Load Test Tools, Smart Sheet Project Management Tracking Tool, QA Traq, Traqroot, JIRA, MS Visio,
Governance Risk Compliance Tools	Expertise in RSA Archer, Agiliance/Risk Vision GRC/Oracle e-GRC/Cyberark Ver 9.3.0

Professional Experience Details-

Bank Of The West, City Of Industry, CA **March 2016-Till Date.**
Cyber Information Security Program-IT Application Implementation and Support
Enterprise Governance Risk Compliance & Information Security

Responsibilities:
Cybersecurity/Threat/Vulnerability-Implementation/Remediation with RSA Archer Development/Administrator on demand Solution Design/Application Configuration,fixing Identified/Reported Vulnerabilities,generating vulnerabilities alerts.Identifying Vulnerabilities by using Qualys Scanning tools for Production/UAT/Test Hosted-Database Server, Web Server, Application Server, Citric Servers, Production Server, User Acceptance Servers, QA Servers, Development Servers,Active Directory, Domain Controller.Analyzing scheduled weekly/daily scan reports,Assigning priorities categorization vulnerability alerts through an automated process at Enterprise Level for individual Application Owners Validating result from Quays Scan Reported, Bank domain,DMZ domain, Workstations, ATM, External Scan, Internal Scan,Remediation based on Bank SLA's,Managing Enterprise Bank IT Application, Security Patches Management Java Vulnerabilities Remediation Plan Projects.Communicating with various Team/Business/Customer day to day, Platform Services,NEO Security,Solution Delivery,Endpoint Management,Enterprise Information Security,Network Security, Business Users, IT-Audit Team, Governance Risk Compliance Team,Publishing the milestones/Score Cards Quarterly basis, Shavlik Patches, Big Fix Patches, Red Hat patches,Certificates Transfer Ownership, Firewall, Security Group Policies, Disaster Recovery Plan,Maintaining CyberArk-password activity for various Server Authentication.

- Identified Vulnerabilities and Remediation Approaches for IT Application Implementation & Support, Email Notification various AIS Team, Weekly/Monthly Vulnerability Management Meeting Schedule.
- Reviewing organization's computing environment and applications using existing policies and standards which are derived from NIST 800-171, Control Implementation Summary (CIS)
- Gramm-Leach-Bliley Act, General Data Protection Regulation, Data Leakage Prevention controls
- Coordinating with business unit Subject Matter Experts (SMEs) to drive security architecture reviews.
- Conducting security program reviews in cooperation with CSO
- Defining and reviewing the security standards and policies of the organization
- Promoting a culture and awareness of cyber security throughout the business
- Cyber risk and mitigation strategies,Federal Risk and Authorization Management Program (FedRAMP)
- Qualys based-creating remediation actions from web application vulnerability reports
- Security approach ability to communicate security requirements across all levels of the Bank.
- SharePoint Site Enterprise Access Management-Security Reports, DCR Monthly Reports
- Supporting Max Finance Application,Equipment Finance Division-Web Portal for Production Support/UAT.
- Managing Cherwell System with various Ticket/SLA approach.
- Identity Access Management,PingOne,NetIQ,Oracle Identity Manager, IT First Line Defence,MRAM,Legal & Regulatory
- Implementation of Threat, Incident,Vulnerability Management Solutions,CIS Controls/Benchmarks
- Endpoint,Cloud,Network,Firewall Security,Burpsuite,Firebug,AppScan,HPWebInspect Tools,Checkpoint,Fireeye
- Authentication NTLM,Kerbores,Digest,Basics,OAuth 2.0 protocol

BNY Mellon, Pittsburgh, PA **Oct 2015 – March 2016.**
RSA Archer - Cyber Security & Threat, Vulnerability Manager
Enterprise Governance Risk Compliance & Information Security
Working as a Vulnerability Manager with RSA Archer development to design/configure/resolve and fix the Vulnerability Alerts resulting from Qualys Scan Reporting, External Scan, Internal Scan, Remedy, BladeLogic which has been reported in the Production environment.

Involved with Security Incident Management Operations, Threat, Vulnerability Management Solutions, Finding Application, Remediation Application, validating Workflow, Notifications, Data Driven Events, Business Calculations, customizing the solutions using Application Builder, designing fields, creating and evaluating Sub Forms, designing i-views, Reports, Dashboards, Roles Access Permissions up to the Archer administration level, creating Reports/Validating Report, Data feed, manage workspaces, manage Packaging, validating all the issues on Development and QA Environment and then moving smoothly on Production Environment for various On Demand Application Management, Facilities and Application, Policies, Control Procedures/Risk Framework.

Responsibilities:

- Strong knowledge of operating systems administration (Unix/Linux, Windows), configuration management, engineering and architecture.
- Strong knowledge of network and firewall administration, networking, routing protocols, telecom network
- **Experience using security incident and events monitoring systems**
- Understanding of TCP/IP Networking including basic UNIX system level network troubleshooting skills
- Knowledge of various remote connection (RDP, Putty, Telnet, SSH, SFTP)
- Knowledge of regular expressions and data manipulation, scripting language (Perl, Python) and MySQl desirable.
- **Receive enterprise assessments of threats and vulnerabilities reports, determines deviations from acceptable configurations and security controls, assesses the level of risk, and develops and/or recommends appropriate remediation strategies**
- **Coordinate actions to remediate vulnerabilities on distributed applications, revising, updating and providing documentation as required.**
- **Maintain thorough knowledge of cybersecurity operations**, **and potential defensive capabilities for countering cyber threats to distributed applications.**
- Lead, execute or participate in parallel, pilot and other system test phases prior to implementation to ensure accuracy and completeness.
- Research, prepare detailed specifications, define designs, develop tests, debug, install, and modify computer software in various platforms in a complex and integrated systems environment.
- Develop and documents project plans, budgets and schedules.
- Provide technical expertise in the examination and definition of objectives for existing or proposed systems and in the design of improved systems utilizing information services. Provides technical assistance to staff including interpretation of specifications.
- Research new developments in hardware and software. Maintain currency in techniques and tools enabling system proficiencies and performance improvements.
- **Evaluate and recommend various technical solutions to meet requirements.**
- Develop proposals including systems, consulting services, benefits and costs.
- Provide system configurations and interface strategies.
- Perform systems integration testing and user acceptance testing as required by software development lifecycle.
- Manage multiple projects and may lead project teams.

Deloitte, LLP @ Commonwealth Of PA, State Government, Harrisburg, PA **July 2015 – Sept 2015**
RSA Archer SME
Enterprise Governance Risk Compliance & Risk Advisory/Information Security/Forensic Analysis

Responsibilities:

- Worked as a RSA Archer SME to design/configure/resolve and fix issues which has been reported in Production for Security Incident Management Operations and Threats.
- Determined vulnerability solutions, validated all the issues on Development and QA Environment and then moved smoothly to Production Environment.
- Worked as **Technical Business Analysis** for Threat and Vulnerability Management, Risk Management, Facilities and Application, Policies, Control Procedures/Risk Framework, Tenable RSA SecurID
- Implemented Vulnerability management Solutions from getting Scanned vulnerabilities to various Government Agencies and importing via Data feed using http/API Integration method.
- Implemented various security NIST,COBIT controls
- Cyber Forensic Analysis Tool Encase, Access Data, FTK, DEFT,HXD,CAINE,File Signature,Registry Analysis, Volatility
- Forensic Cyber Analysis-Live Acquisition, Imaging, Tampered, Evidence,MD5SHA1,Write Blockers, Virtual Memory

Infosys@Aetna, Hartford, CT **Apr 2015 – June 2015**
RSA Archer Developer
Governance Risk Compliance, Information Security.

Responsibilities:

- Worked as a RSA Archer Developer to resolve and fix issues which has been reported in Production.
- Involved with Business Continuity Management, Incident Management and Vendor Risk Management Solutions.
- Involved with **Audit Project Management** using a risk-based scoping methodology along with **Disaster Recovery Risk Management.**
- Functioned as a **Technical Business Analysis** for Threat and Vulnerability Management, Risk Management, Compliance Management, Policy Management, Audit Management, Facilities and Application.

HCL Technologies, Noida India **Dec 2014 – Mar 2015**
RSA Archer Consultant
Governance Risk Compliance, Information Security

Responsibilities:

- Worked as **RSA Archer GRC Consultant/Administrator.**
- Managed users and groups, managed roles and access permissions, managed applications, managed i-Views, managed Dashboards, created Application layout for various solutions like Vendor Risk Manager, Compliance Manager, Enterprise Risk Manager, Policy Manager Solutions, Business Continuity Management, Incident Management Plan and Audit Management.
- Created multiple email notifications, managed Workspaces, Data Driven Events and Business Calculations.
- Customized the solutions using Application Builder, designed fields, created and evaluated Sub Forms, built i-Views, built reports, dashboards, managed role access and permissions for various On Demand Application.
- Debugged production issues on QA/Development environments and resolved all reported issues on the production/development/QA Servers with complete business analysis and documentation

Agiliance/Risk Vision, Hyderabad-India/Sunnyvale-USA

Mar 2008 – Nov 2014

Governance Risk Compliance Lead & Information Security

Agiliance/Risk Vision System runs an enterprise-class server application to monitor and enforce policies, send and receive information from client "agents" and connectors, process, display all compliance and security risk data, and perform all other operations requested by users. Agiliance uses a relational database to store all policy compliance and security risk information and results, evidence, survey and questionnaire responses, and provides a web-based console application. Users can perform all operations to monitor and control Agiliance operations based on the roles and associated permissions that users have been granted by the Agiliance system administrator and need to connect the Agiliance Appliance to a network that has TCP/IP connectivity with the systems and computers you wish to monitor and manage.

Supported numerous clients on governance risk compliance and information security. Clients included KPMG, State Street Bank, DnB Norway, Fiserv, Safeway, Deutsche Bank, First Energy, HighMark, Exelon, HHS, CIT, Etrade, Bell Canada, etc.

Responsibilities:

- Managed **Vulnerability Assessment using IBM Security AppScan /Vera code Source Code Tool**
- **Conducted Compliance Manager, Policy Manager, Enterprise Risk Management, Vendor Risk Management**
- **Conducted Threat & Vulnerability Management, Incident Management, Automated Data Collection, Security Assessment**
- Installed multiple configurations of Windows, Linux and Microsoft server software including Microsoft Active Directory.
- Configured Servers with Apache, Tomcat, MySQL, Oracle on Windows for 32 and 64 bit platforms.
- Maintenance of Information Security standard ISO 27001:2005.
- **Hands on experience in Information Security Risk Management based on BITS framework, COBIT, NIST 800-30, ISO 27005 etc,** Incident Management Plan, Disaster Recovery Process Plan.
- Implemented Role Based Access Governance and HIPPA Compliance for KPMG. Health Insurance Portability and Accountability Act (HIPAA) Security Rule NIST-800-66 specifically focuses on the safeguarding of electronic protected health information (EPHI). All HIPAA-covered entities, which include some federal agencies, must comply with the Security Rule, which specifically focuses on protecting the confidentiality, integrity, and availability of EPHI.
- Implemented Common Control Framework Correlated controls across multiple regulations, frameworks and programs enabling an organization to test once, and comply multiple times.
- Automated Control Framework: Tested and reported control failures automatically without human intervention and without the use of surveys.
- Policy Mapping Framework: Mapped controls to policies and vice versa, enabling an organization to institute governance and track the automation and execution of policies against specific controls.
- Risk Mapping Framework: Mapped controls to standard or custom risk catalogs that further map to a risk management engine, enabling an organization to analyze the true business impact of control failures.

OutworX,Pune-India, Guardian Edge **Apr 2007 – Feb 2008**
Sr SOA Engineer

GEHD: (Guardian Edge Hard Disk) is the most effective way to protect data on corporate laptop and desktop computers. This software offers: Full disk encryption, meaning that the software encrypts every sector on a computer hard drive, including temp files, system files and unused disk space.

Centralized management control over hard drive encryption settings, password settings, auditing and enforcement of information security policies Seamless integration with Windows Server 2003, Active Directory and all other Encryption Anywhere solutions access control for local and network resources using pre-Windows authentication. Robust recovery options, including Authentic-Check® self-service password recovery and reset tool that eliminates the need for Help Desk support due to forgotten passwords.

SEE-FD: (Symantec End Point – Full Disk Protection) is a product same as GEHD of Guardian Edge. This product has been collaborated with Symantec and has been designed as per requirement of Symantec.

Responsibilities:

- Involvement in Preparation of Testing Strategy Document
- Preparation of Test Plans/Test Cases
- Bug reporting and maintaining bug database
- System Testing, Regression Testing and Build verification
- Resolved bug issues with developers
- Installation and Configuration of the Product/Application

Technology- Java/J2MEE, JSP, XML, HTML, Java Script
Operating System- Windows-XP/2003/Linux/Unix for Deployment and Testing

OutworX – Noida-India-TriCipher Inc, USA **Oct 2005 – Mar 2007**

SQA Engineer

TACS is a high assurance authentication system, which can issue easy to use credentials ranging from zero footprint solutions to strong, token-based solutions. The entire user sees is a login screen that requires a user name and password like they use today. TACS makes strong authentication easy to deploy. TACS stores credential data in a highly secure FIPS-rated appliance, ensuring both regulatory compliance and high assurance. TACS is designed for high availability and scalability.

Responsibilities:

- Bug reporting and maintaining bug database
- System Testing, Regression Testing and Build verification
- Resolved bug issues with Program Managers [USA]
- Reviewed Technical specifications
- Netscape/Mozilla with Linux, Safari/Firefox with MAC
- Resolved issues with Technical Support Team

Technology- VC++, Dot Net, Java/J2EE, JSP, XML, HTML, Java Script, Free BSD Database
Operating System- Windows-XP/2003 Server/Mac/Unix/Linux for Testing

OutworX – Noida-India, Lattice 3D, USA **Apr 2004 – Sept 2005**

Software Engineer

Plug in-Based Application (Desktop Application) through which user can get the Engineering Analysis and Measurement/Viewing of any 3D/2D/Images/CAD/GIF. Engineers and manufacturers can perform design review, simulate assembly processes, automate creation of 3D parts lists / BOM's and create animations with even the largest 3D assemblies. Lattice's standards based XVL (extensible Virtual world description Language) technology provides secure, highly accurate and compressed 3D files that can be used, shared and easily supported by partners, suppliers, and internal departments in a lightweight browser-based solution.

Responsibilities:

- Development and execution of Test Plan/Test Cases.
- Identified the Test Requirement of the Application.
- Reported Bug Defects and Resolving Customer Issues.
- System Testing and Integration Testing and Regression Testing,
- Reviewed the Functional and Technical Specifications.
- Managed all Phases of Build and Release Activities.
- Configuration Management Methodology.

Technology- VC++/MFC/Dot Net/Microsoft Visual Studio, Active-X-Controls, Corba
Operating System- Windows-XP/2003/Linux for Testing