SURAJ VERMA

CONTACT NUMBER: +91 9619018266;
ADDRESS: B2/101,LOK RAUNAK CHS, MAROL, ANDHERI EAST
MUMBAI, MAHARASHTRA

OBJECTIVE

Seeking a career in an international and national industry, where my learning skills, education and Information security management abilities would be an advantage to the growth of my employer and myself. My keen interest in Information Security that would be my key driver toward achieving my goals.

SKILLS

Information Security Management, GxP, GISC, ICS, ISO 27001, PCI DSS, PA DSS, Audit, Risk Management, GDPR, CAMP, Cloud Security Assessment (CSA-CSM), Vulnerability Management, Security Due Diligence, GRC, SAP GRC, Project Management, Vendor and Partner Mgmt.

EXPERIENCE

Total Full-Time Work Experience: - 13 Years

Previous Employer Name: - EClinicalWorks India Pvt Ltd(www.eclinicalworks.com)
Designation: - Software Specialist
Previous Employer Name: - Fractal Analytics Ltd. (www.fractalanalytics.com)
Designation: - Officer
Previous Employer Name: - HCL (www.hcl.com)
Designation: - Specialist (Information Security Consulting)
Previous Employer Name: - SurePrep India Pvt Ltd(www.corp.sureprep.com)
Designation: - Senior Security Analyst (InfoSec-Development)
Previous Employer Name: - SurePrep India Pvt Ltd.
Designation: - Manager (InfoSec)

Present Employer Name: - Bayer
Designation: - Security Architect
Duration: - September 2021 - Present Employer

Responsibilities: -

- Developing security policies, standards, and processes to protect the Company's information resources.
- Planning all the audits, creating audit schedule, communicating with external auditor.
- Keeping track of all the audits findings and observation, suggesting resolution to audit finding to departments across organization.

SURAJVRM@YAHOO.COM
+919619018266
HTTPS://WWW.LINKEDIN.COM/IN/SURAJ-VERMA-11481037

- Performing risk assessment, rating the risk as per their values and creating the treatment plan
- Managing ISO-PCI-SOC2 TII Certification and European Union GDPR
- Creation, development and review IS policies, procedures, guidelines and SOP's
- Plan and conduct IS Audits.
- Plan and conduct IT General control reviews.
- Create audit checklist, audit program, and management audit work papers
- Manage task allocation, ensuring the quality of the deliverables in line with industry standards and best practices Audit preparation & facilitate auditor as per IS audit calendar
- Planning and execution of audit in line with annual audit calendar
- Prepare the report of audit findings, observations, gaps etc.
- Ensure closure of the nonconformities with appropriate measures [corrective/preventive]
- Knowledge of IS controls around servers, networking devices like firewalls, routers & other technical controls
- Plan and conduct various audits like desktop audit, end user audit, etc.
- Understanding IS controls and processes related to Information Security management and COB
- Review and tracking of issue closure and provide metrics
- Support additional due diligence required for new engagement
- Submission of reports / MIS
- Installing critical security patches within one month of release.
- Reviewing public facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes.
- Immediately revoke access for any terminated users.
- Remove / disable inactive user accounts at least every 90 days (through Group policy setting)
- Store Physical access control logs for at least three months, unless otherwise restricted by law.
- Review security of media backup site or commercial storage facility annually.

SURAJVRM@YAHOO.COM

+919619018266

HTTPS://WWW.LINKEDIN.COM/IN/SURAJ-VERMA-11481037

- Promptly back up audit trail files to a centralized log server or media.
- Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization,
- Retaining audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).
- Verifying that internal and external scanning is occurring on a quarterly basis.
- Performing internal and external penetration test annually and after any significant changes to the environment.
- Configuring the file integrity monitoring software to perform critical file comparisons at least weekly.
- Conducting Risk Assessment and internal VAPT using tool such as nessus, qualys guard and burpsuit.
- Creating hardening procedure for application, network and server devices
- Perform issue categorization and in-depth analysis of security events. Conduct all necessary follow-up actions of vulnerability and/or security incident resolution.
- Maintaining security elements at each stage of Software development life cycle.
- Design and implement the security best practices along the entire Software Development Life Cycle (SDLC), collaborating with the development teams.
- Lead the creation of the security side of the Software Development Life Cycle.
- Participate in the entire development cycle with the IS team to ensure the right security is in place.
- Keep track and documentation of all applications being developed or implemented by IS or IT Team.
- Develop/integrate cybersecurity designs for applications with multilevel security requirements or requirements for the processing of multiple classification levels of data.
- Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the Software Development Life Cycle (SDLC).
- ·Perform threat modelling, design reviews and code reviews as part of the development lifecycle.

SURAJVRM@YAHOO.COM

+919619018266

HTTPS://WWW.LINKEDIN.COM/IN/SURAJ-VERMA-11481037

- Perform security architecture and design reviews of systems and applications developed
- Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
- Identify and prioritize critical business functions in collaboration with organizational stakeholders.
- Perform security reviews, identify gaps in security application architecture, and develop a security risk mitigation plan.
- Act as advisor in the definition and documentation of how the development of new applications or new interfaces between systems impacts the security posture of the current environment.
- Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.
- Preparing the technical documentation, explaining the solution to the daily incident and preparing other knowledge base data from the s/w provider across different business formats
- Management of user accounts and providing access controls to client data.
- Create internal Plans for system software and hardware maintenance, evaluate, test and integrate upgrades to operating systems, software and other applications
- Training the client about functionality of software and solving their issues
- Coordinate security projects and acts as a liaison between IT Security, process owners and system managers.
- Responds to security incidents, providing assessment of impact severity and types of incidences being addressed. Coordinates resolution efforts and prepares reports of findings.
- Designing IT policies and procedures which comply all the requirement stated in ISO 27001 , NIST and PCI DSS 3.0
- Designing and Performing Risk assessment document for all the format within the organization, Identifying the assets under high risk and timely treating those risk
- Gather security metrics and report them to management.
- Maintain security documentation and diagrams.

SURAJVRM@YAHOO.COM

+919619018266

HTTPS://WWW.LINKEDIN.COM/IN/SURAJ-VERMA-11481037

- Performing Cloud infrastructure assessment based on CSA FRAMEWORK
- Client Due diligence activity and implementing security control based on client MSA
- Perform security reviews, identify gaps in security application architecture, and develop a security risk mitigation plan.
- Act as advisor in the definition and documentation of how the development of new applications or new interfaces between systems impacts the security posture of the current environment.
- Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.

EDUCATION

MASTER OF
COMPUTER APPLICATION • 2013 • SMU UNIVERSITY

BACHELOR OF SCIENCE
(INFORMATION TECHNOLOGY) • 2007 • MUMBAI UNIVERSITY

CERTIFICATION
ISO 27001 INFORMATION SECURITY MGMT. SYSTEM LEAD AUDITOR
ISO 19011 AUDIT MANAGEMENT


SURAJVRM@YAHOO.COM


+919619018266


HTTPS://WWW.LINKEDIN.COM/IN/SURAJ-VERMA-11481037