|  |  |
| --- | --- |
|  |  |

**IT Risk Analyst**

Name: Anil Kumar Dirishala

Contact :[347-762-6896](tel:(347)%20762-6896)

Email :[adirishala@gmail.com](mailto:adirishala@gmail.com)

Experienced Information Security and Technology professional with over 5+ years of experience in information system governance, engineering, and management of cybersecurity. This includes, but not limited to, risk management, auditing, policy development and compliance.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Professional Abridgement**

* Information Security Officer (ISO) – Information Security, GRC Consultant with approx. 5 years of experience in Governance, Risk, Compliance & Audit –ISO 27001, PCI, HIPAA, SOX etc. Information Security & Network security functions.
* Participate in audit, compliance, remediation, testing and assessment activities
* Perform and assist with Risk Assessment activities
* Extensive exposure to developing and reviewing cyber security policy and system/network security packages.
* Assist the ISSO with the generation of Waivers, POA&M closure packages and Authorization packages for submission to the Authorizing Official
* Evaluate, maintain, and communicate the risk posture of each system to executive leadership and make risk-based recommendations to the Chief Information Security Officer(CISO)
* Thorough understanding of multiple security frameworks to include DIACAP, RMF and PCI-DSS.
* Hands-on experience with eMASS, DISA STIGs and SCAP reports in DoD environments.
* Proven expertise in performing the management of information systems, technologies & security audits for evaluating the effectiveness of operations and compliance with applicable laws & regulations
* Prepare written responses to routine security and compliance inquiries by preparing, modifying documents including correspondence, reports, drafts, memos and emails
* Provide development guidance and assist in the identification, implementation, and maintenance of compliance policies, procedures and work instructions
* Involve in the security awareness and training of staff on HIPAA requirements as it relates to information technology
* Conduct IT controls risk assessments that include reviewing organizational policies, standards and procedures and provide advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard

**Certification and Education**

Master of Science in Cyber Security

Diploma in Information Assurance and Security (Level 7)

**Apple Inc. (Dec 2016 - Present)**

**Sunnyvale, CA**

**Information Security Auditor**

* Reviewed assigned Risk Management Framework (RMF) controls and developed appropriate supporting documentation.
* Reviewed and assessed information security events and Improved Security Controls of Information Security Management systems (ISMS) based on ISO27001 standard.
* Develop and implement information security internal audit program in accordance with established corporate and regulatory standards.
* Manage implementation of Information Risk Management approach based on ISO/IEC 27005:2008 standards.
* Oversee all aspects of internal audits. Set deadlines, assign responsibilities, and monitor and summarize progress of internal audits.
* Build and maintain working relationships with team members and other departments involved in the audits. Prepare reports for upper management regarding status of audits.
* Analysed threats and vulnerabilities to determine their impact upon IT systems.
* Developed policies and procedures for PCI and ISO compliance.
* Conducted System Security Assessment to support Department of Labor (DOL) Cloud Services
* Prepared recommendation reports that are available to System Owners to remediate identified vulnerabilities during the risk assessment process
* Conduct quarterly Information Security Management meetings with IT management to include client, internal and external audit findings; risk assessments; improvements to security and changes that can affect security.
* Analysed and updated System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security Test and Evaluation (ST&E) and the Plan Of Action and Milestone (POA&M)
* Ensured quality analysis of audit control.
* Created an architectural design for the delivery of Information Security solutions around Risk and compliance in the cloud.
* Examined events logs for irregularities. Identified irregularities are then reported as incidents. The incident response process is then initiated to mitigate these irregularities
* Provided customer service with higher standards to enhance the client experience

**Pitney Bowes** **(Oct 2015- Nov 2016)**

**Shelton, CT**

**Information Security Auditor**

* Developed, reviewed and updated Information Security Policies, System Security Plans (SSP), and baselines in accordance with NIST, FISMA, OMB A130.
* Developed, evaluate and implemented information security governance processes, including policies, standards, procedures and risk management practices.
* Performed operations such adding and removing user account and Computers from Active Directory Domain.
* Develop systems that assist the organization to secure the CIA by categorizing and selection of controls using NIST SP 800-60, 800-53 and FIPPS 199 and 200
* Tracked authorization expirations for different system including general support systems (GSS) and Major Applications (MA)
* Worked with IS auditor and ISSO to remediate all identified security vulnerability detected.
* Responded to network security incidents including data breaches, viruses, and unauthorized access attempts.
* Experience in deploying and implementing AWS infrastructure consists of supporting users, EC2 instances.
* Assessed incoming threats and developed plans to close loopholes.
* Experience in using VMware Vsphere administration of virtualized servers using the AWS cloud integration .
* Conducted vulnerability assessments to evaluate customers' security posture for Connection
* Performed compliance activities and testing including recertification and processing documentation

**Hexagon Solutions (Jan 2012- July 2015)**

**India**

**Information Security Analyst**

* Performed Computer Security Incident Response activities for a large organization, coordinates with other government agencies to record and report incidents
* Monitored and analysed Intrusion Detection Systems (IDS) to identify security issues for remediation
* Recognized potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information
* Evaluated firewall change requests and assess organizational risk.
* Provide guidelines for implementing secure systems to customers or installation teams.
* Assisted with implementation of counter-measures or mitigating controls.
* Ensured the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices.
* Performed periodic and on-demand system audits and vulnerability assessments, including user accounts, application access, file system and external Web integrity scans to determine compliance.
* Design the Web listeners and firewall policy rules on reverse proxy to allow the Internet users to access the Internal servers/ resources through Internet.