**Razi Mohd**

**727-637-4271**

[razi.mohd728@gmail.com](mailto:razi.mohd728@gmail.com)

Over all 10 years of experience in Technologically sophisticated Information Security professional, versatile in building and maintaining a security program. Hands on with managing risks, vulnerabilities, compliance and auditing.

**Core Advantages:**

* CISSP, CISA, Masters in Information Security
* Vulnerability and Risk Management
* Third Party Risk Management
* Security Awareness, Records Management, M & A.

**Academic Qualifications:**

* *Bachelor’s in E-Commerce*
* *MS in Information Security*

**Professional Certifications:**

* ***CISSP*** *(Certified Information Systems Security Professional)*
* ***CISA*** *(Certified Information Systems Auditor)*

**Professional Experience:**

**Larsen and Tourbo, Dallas, TX                                  August 2019 – present**

**Sr. Information Security Analyst**

**Responsibilities:**

* Led the information assurance program, leveraging expertise in Network Access Control (NAC) to facilitate assessment reviews of individual business units and supplier compliance using Security Studio.
* Identified and reported compliance gaps to key stakeholders, integrating expert knowledge for comprehensive remediation actions via ServiceNow (SNOW).
* Proactively identified and addressed all instances of overlapping questionnaires within silo compliance program efforts (SOX, PCI, HIPAA, state regulations like NYDFS, etc.).
* Established an efficient central evidence repository on Sharefile, ensuring streamlined utilization across multiple regulations and standards without duplicating work.
* Provided crucial support to team members and business processes, managing the lifecycle and inventory of critical technology assets. Applied monitoring, enumeration, and classification techniques for various regulatory and compliance information assets, utilizing skills in Mcafee and Symantec Endpoint protection (SEP).
* Implemented and monitored security controls for I.T. systems and major applications in the cloud environment for Azure, AWS, and Sales Force (IaaS, SaaS, PaaS) using FedRAMP guidelines.
* Managed compliance program scope effectively, including 1st level triage of consultative requests.
* Performed Vulnerability scanning on our network and make sure that vulnerabilities are addressed.
* Strong understanding of enterprise, network, system/endpoint, and application-level security issues and risks.
* Consulted with stakeholders and suppliers to ensure compliance for new and existing business/technology solutions. Addressed regulatory and contractual control requirements (e.g., PCI, HIPAA, state regulations).

**Amazon, Seattle, WA                                           August 2018 – July 2019**

**Sr. Information Security Engineer (Contract position)**

**Responsibilities:**

* Started with performing risk assessments, enterprise-wide third-party Risk Management using Censinet, and was responsible for third party risk, compliance and policies.
* Moved into the role of conducting due diligence and risk assessments for mergers and acquisitions.
* Performed Vulnerability scanning on our network and make sure that vulnerabilities are addressed.
* Launching Amazon EC2 Cloud Instances using Amazon Machine Images-AMIs (Linux) and Configuring launched instances with respect to specific applications.
* Create CyberArk Safe's and add system and application id's to specified Safe vaults
* Created training and reinforcement materials using TalentLMS to enhance security awareness across Amazon employees and acquisitions globally.
* Took charge of enterprise-wide Phishing exercises using Cofense to mitigate internal threats.
* Developed Architecture and Design for implementing CyberArk solution in distributed environment in order to manage application and service credentials
* Collaborated with the helpdesk and Incident Response team to design and deliver sessions tailored for specific employee groups.
* Ensured meticulous records management and conducted annual certification throughout the company.
* Resolved CyberArk issues in CPM communicate with host to reconcile credentials.
* Collaborated closely with the archiving partner to supervise all retention policies.

**Franciscan Alliance, Beech grove, IN                     May 2017 –June 2018**

**Information Technologist (Contract position)**

**Responsibilities:**

* Conduct audits on risk assessments for biomedical devices, vendors/contractors, and internal projects, utilizing tools such as Nessus to enhance the evaluation process.
* Perform Vendor posture assessment before approving them to provide services.
* Request information using vendor questionnaire and MDS2 order to perform the risk assessment  
  on the bio-medical devices and on new project implementations.
* Ensure appropriate information security and business continuity controls exist to protect sensitive  
  information.
* Utilize the vulnerability management tool Tenable to identify, assess technology risks, implement mitigating controls, and explore opportunities for enhancing control effectiveness.
* Continually seek ways to raise the bar and ensure higher levels of standards across the risk and compliance domain and make sure implementations are done as per Franciscan policies and procedures.
* Support overall company wide effort in maintaining primarily HIPAA compliance.
* Perform risk assessment on medical devices following NIST 800-53 framework and applicable  
  methodologies.
* Utilized JIRA to ensure issues are managed to closure and deadlines are met in a timely fashion.

**HSBC Financial, Hyderabad, India Aug 2012 – June 2015**

**Cyber Security Analyst**

**Responsibilities:**

* Successfully created and implemented comprehensive security policies for the banking industry, demonstrating a deep understanding of industry-specific risks and regulatory requirements.
* Conducted thorough risk assessments to identify potential vulnerabilities and developed strategic security policies to mitigate risks, ensuring the protection of sensitive financial data and customer information.
* Proven track record in ensuring compliance with industry standards and regulations, including but not limited to PCI DSS, GLBA, and other financial regulatory frameworks, through the development and enforcement of robust security policies.
* Organized the development of incident response plans, outlining clear procedures and protocols to address security incidents promptly and effectively, minimizing potential damage and ensuring a swift recovery.
* Implemented training programs to educate employees on security policies and best practices, fostering a culture of security awareness and compliance throughout the organization.
* Demonstrated commitment to staying abreast of emerging security threats and technologies, regularly updating security policies to align with industry best practices and evolving cyber threats.
* Collaborated with cross-functional teams, including IT, legal, and compliance departments, to ensure alignment of security policies with overall organizational goals and objectives, fostering a cohesive and integrated approach to security management in the banking sector.