**PORTIA ASIKUMAH**

 Missouri City, Texas, United States portiaasikumah@gmail.com 8326611594

**Professional Summary**

Over **5 years** of successful experience in cybersecurity industry and ability to work in a fast-paced enterprise environment. An excellent grasp of cybersecurity within an enterprise government cloud environment, able to apply FedRAMP, and RMF security practice expertise across complex cloud architectures. Security lead who provides regulatory, compliance, Risk Management and Cybersecurity guidance.

**Core Competence**

Continuous Monitoring process and relationship with the FedRAMP, DoD Authorizing Official. NIST-based system security assessments, privacy assessments, continuous monitoring, and/or other Assessment and Authorization (A&A) activities, Risk Management Third Party Vendor Risk Management, Vulnerability Management reporting, Archer, VPN. Security Lead with an advanced knowledge, and understanding of private, commercial and/or government community clouds like Microsoft, and other regulatory framework which includes; NIST 800 Series, SOC1&2, HIPAA. A vast experience in Microsoft office suite; (Word, Excel, PowerPoint, Outlook Visio) and Mac Platforms, Windows 10, Adobe, Dropbox, Active Directory, Security Score Card, Qualys, Crowdstrike, SecureWorks, Splunk, RFP’s, Loopio, Zendesk, Pipedrive.

**Work Experience**

**CVS Health**

**Senior Security Risk Management Analyst 01/2022 – Date**

* Manage, track and oversees risk-based vulnerability aligned in Crowdstrike and SecureWorks to make sure that malicious Ips are blocked, review or monitored.
* Perform risk analysis, risk profiling of systems and analyzing the adequacy of controls implemented to mitigate identified risk.
* Ensures data integrity and accuracy of vulnerability data within our controls.
* Scan, report and track identified risk/vulnerabilities and produce detailed reports or assessment to team.
* Managing and facilitating the incorporation of evidence, scans and produce detailed report or assessments.
* Utilize tenable controls to discover vulnerabilities and implement POA&M to remediate and mitigate the vulnerabilities identified.
* Ensure effective and efficient execution of assigned project tasks in conformance with professional and departmental standards.
* Collects and reviews the appropriate security controls from SOC1 & SOC 2 to answer vendor security questionnaires.
* Manage the security vulnerabilities and risk across the enterprise environment including identifying, support application/system owners to manage and remediate vulnerabilities.
* Review and monitor security questions/RFPs from business partners
* Monitor log flow to Splunk, verify host stat counts, webproxy and syslog counts.

**VA Claims Insider**

**Information Security Analyst**  **10/2020 – 07/2021**

* Ensured information systems undergo appropriate validation and accreditation processes to meet Federal Information Security Management Act compliance
* Managed categorization of security controls using FIPS199 and SP 800-60, System Security Plan, Incident Response Plan, Privacy Threshold Analysis, Interconnection Security Agreements, POA&Ms, Vulnerability Scans, Configuration Management Plans, etc.
* Contributed to the coordination of third-party control assessments and audits in accordance with the scope of security and privacy assessment plans
* Provided expert level guidance to continuous monitoring and Continuous Diagnostics and Mitigation (CDM) programs by reviewing security documentation
* Managed audit logs, vulnerability scans, configuration baselines for security and environment changes and reports the security and privacy posture to the Authorizing Official, supervisor, and senior leadership
* Developed and implementing cybersecurity incident response plans and provides cybersecurity awareness and training
* Performed risk assessments, identify IT controls for significant processes.

**HealthHelp**

**Information Security Specialist 02/2019 – 10/2020**

* Recommend programmatic and technical directions and operate with a high degree of independence in matters relating to the investigation, impact, and analysis of decisions regarding risk, and measures for computer and network security.
* Lead the development and implementation of the system-wide risk management function of the information security program to ensure information security risks are identified and monitored.
* Internally assessed, evaluate and make recommendations to management regarding the adequacy of the security controls for the hospital’s information and technology systems.
* Lead the system-wide information security compliance program, ensuring IT activities, processes, and procedures meet defined requirements, policies and regulations.
* Developed and implement effective and reasonable policies and practices to secure protected and sensitive data and ensure information security and compliance with relevant legislation and legal interpretation.
* Coordinated and track all information technology and security related audits including scope of audits, colleges/units involved, timelines, auditing agencies and outcomes. Work with auditors as appropriate to keep audit focus in scope, maintain excellent relationships with audit entities and provide a consistent perspective that continually puts the institution in its best light. Provided guidance, evaluation and advocacy on audit responses.

**FortBend ISD**

**Information Security Analyst 01/2016– 03/2019**

* Lead the development, assessment, and analyzing of cyber security documentation for internal and tenant service offerings information systems in accordance with FISMA, NIST RMF for Federal Civilian Agencies, RMF for DoD, FedRAMP, and departmental standards.
* Performed vulnerability/risk assessment analysis to support certification and accreditation. Provides configuration management (CM) for information system security software, hardware, and firmware. Manages changes to system and assesses the security impact of those changes.
* Developed and maintain system security plans (SSP), contingency plans (CP), incident response plans (IRP), configuration management plans, security control requirements and assessments, Plan of Action and Milestones (POA&M), and training requirements
* Ensured that existing business environments adhere to Federal Information Assurance policies and procedures to acquire and maintain an Information System's Authority to Operate (ATO) under the Federal Information Security Management Act (FISMA) and other client specified regulatory/Security standards
* Effectively mitigated risk by identifying security deficiencies and deviations from policies and standards and providing Quality Assurance.

**Education**

8/11-12/15 University of Texas at San Antonio, San Antonio, TX Bachelor of Science in Public Health, Epidemiology, & Disease Control

**Certifications**

CISM

CompTIA Security+

Certified Scrum Master (CSM)

CISSP – In progress