Information Security Analyst Information Security Analyst Information Security Analyst - Smart Think Inc. MD Baltimore, MD Analytical, performance-driven, highly motivated Information Security Professional experienced in Security Assessment and Authorization process, from initiation to continuous monitoring. Knowledgeable in the development of SSP, SAP, SAR, RAR, POA&M, Authority to Operate (ATO), FISMA Reports, Standard Operating Procedures (SOP), in accordance with Federal Agencies and Commercial Organizations policy, to include FISMA, NIST, OMB, ISO, FIPS instruction. Authorized to work in the US for any employer Work Experience Information Security Analyst Smart Think Inc. MD November 2017 to Present Involved with developing, reviewing, maintaining, and ensuring all Assessments and Authorizations (A&A) documentation are included in system security package. Involved with developing, reviewing and updating policies and procedures, audit and compliance with but not limited to RMF, NIST and FISMA. Ensure Implementation of appropriate security control for Information System based on NIST Special Publication 800-53 rev 4, FIPS 200, and System Categorization using NIST 800-60, and FIPS 199. Review and update remediation on (POAMs), in organization's Cyber Security Assessment and Management (CSAM) system. Work with system administrators to resolve POAMs, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Apply appropriate information security control for Federal Information System based on NIST 800- 53A rev4, SP 800-53 rev4, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Work with stakeholders and system application teams to conduct testing, interviews, and collection of artifacts relevant to assessment of security controls. Responsible for ensuring that Security Authorization packages such as System Security Plan (SSP), Plan of Action and Milestones (POA&M), Security Assessment Report (SAR) are maintained reviewed and updated in accordance to NIST guidelines. documentation for Security Control Assessment, vulnerability testing and scanning. Develop and update Security Plan, Plan of Action and Milestones (POA&M). Monitor controls post authorization to ensure continuous compliance with the security requirements. Lolubyte IT Consultant January 2017 to September 2017 Information Security Analyst Coordinate projects that implement security policies, standards, guidelines and procedures to ensure that security is maintained in accordance with FISMA, NIST 800 series. Conducted security control assessment interviews to determine the Security posture of the System and to develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. Performed security control assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Familiar with security scan of systems using vulnerability scanning tools using Tenable Nessus. Analyzed security reports for security vulnerabilities in accordance with the organization Continuous Monitoring Plan and NIST 800-137. Provided recommendations in finding meeting with selection and implementation of controls that apply security protections to systems, processes, and information resources using the NIST family of security controls. Worked with support and security coordination team to ensure compliance with security processes and controls. Responsible for developing Security Authorization documents and also ensures System Security Plan, Security Assessment Plan, Plan of Action and Milestones (POA&M), Contingency Planning and artifacts are maintained and updated in accordance with NIST guidelines. Performed library functions such as archiving and filing of final SA and RA documents, Process/Procedure documents, inventory and maintenance. Validate remediated vulnerabilities. Coordinate the closing of current and backlogged POAM items with internal teams and client. Washington Tech Solution January 2016 to December 2016 Entry Level Security Analyst Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. Conduct security assessment interviews to determine the posture of the System and to Develop a security Assessment Report (SAR) in the completion of the security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization To Operate (ATO), the Risk Assessment, System security Plans, and System Categorization. Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Work with system owners to develop, test, and train on contingency plans and incident response plans. Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. Review and update remediation on plan of action and milestones (POA&Ms), (IACS) system. Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Network Administrator Orange - Cote d'Ivoire March 2012 to December 2015 Establishes network specifications by conferring with users; analyzing workflow, access, information, and security requirements; designing router administration, including interface configuration and routing protocols. Establishes network by evaluating network performance issues including availability, utilization, throughput, goodput, and latency; planning and executing the selection, installation, configuration, and testing of equipment; defining network policies and procedures; establishing connections and firewalls. Maintains network performance by performing network monitoring and analysis, and performance tuning; troubleshooting network problems; escalating problems to vendor. Secures network by developing network access, monitoring, control, and evaluation; maintaining documentation. Education Bachelor in computer science PIGIER CI February 2008 to February 2012 Bachelor's Skills SECURITY (3 years), NESSUS (3 years), ACCESS CONTROL (2 years), APACHE (Less than 1 year), Cyber Security (5 years), Nist (3 years), ACCESS (3 years), Word, Organizational Skills, Excel, Customer Service Certifications/Licenses CompTIA Security+ June 2018 to Present CAP In Progress Additional Information Skills Risk Management, Authentication and Access Control, Vulnerability Assessment, System Monitoring, Regulatory Compliance, Network Security, Nessus, Remedy, Apache web servers, Mail servers, FTP, DHCP, DNS, Red-Hat, SSH, VMware, Virtual box, Red-hat Enterprise Linux (RHEL)

Name: Kimberly Wood

Email: ufrancis@example.net

Phone: 752.442.2964x32664