Lolubyte IT Consultant Lolubyte IT Consultant Lolubyte IT Consultant - Company Authorization To Operate Adelphi, 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. Work Experience Lolubyte IT Consultant Company Authorization To Operate July 2017 to Present 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. Information Security Analyst Smart Think Inc. MD May 2016 to July 2017 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. IT Support Technician / Help Desk Global Aid System - Arlington, VA June 2012 to February 2014 Handle customers' inquiries and complaints. Dispatch and document service orders/trouble reports to appropriate installation and repair service department. Act as the liaison between the customers and installation/service department Negotiate commitment time, technician access arrangement and handle any customer that may be irate or dissatisfied with service. Provided base level IT supports to both internal and external customers. Logged all complaints and inform customers about issue resolution progress. Assigned issues to appropriate support group for thorough support and prompt resolution. Logged defects and verify defect fixes. Supported users having data and network connectivity issue.

Provided first level support to customers before escalation. Cross-trained and provided back-up for other IT support representatives when needed. Displayed exceptional telephone etiquette and professionalism in answering and resolving technical calls. Education Bsc. in Mathematics University of Buea Associate of Science PG community College Skills SECURITY (5 years), NESSUS (4 years), ACCESS (4 years) 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: Benjamin Gray

Email: greenenicholas@example.com

Phone: +1-480-251-5059x638