Security Control Assessor Security Control Assessor Security Control Assessor - TECH CONSULTING LLC Bowie, MD Insightful, results-driven Information System Security Professional with experience in IT Service Management, Risk Management Framework (RMF), Vulnerability Management, Risk Assessment, Security Documentation and System Development Life Cycle (SDLC). A proven project and team lead with aptitude for good customer service, leadership, excellent communication (both oral and written), and presentation skills. Work Experience Security Control Assessor TECH CONSULTING LLC January 2019 to Present Responsible for all phases of C&A to ensure compliance and provide guidance on IT Security requirements assigned to stakeholders. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, NIST 800-53 rev4, FIPS 199, FIPS 200 and OMB A-130 Appendix III, etc. Analyze, assess and recommend security controls for FedRAMP compliance Develop findings reports using knowledge of NIST 800-37 RMF, FIPS 199, NIST 800-34 Contingency Planning, and POA&M management and continuous monitoring. Assist with developing and reviewing compliance reports that clearly identify security findings and proposed remediation strategies. Providing expert guidance in the development or delivery of documents such Authorities to Operate (ATO)s, FIPS 199, FIPS 200, etc. Execute examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4. Test system technical security configuration settings by reviewing Nessus scan results for compliance with industry standards Ensure cyber security policies are adhered to and that required security controls are implemented correctly. Assist the client in categorizing and selecting controls using NIST SP 800 60, 800 53 rev 4 and FIPS 199. Perform the role of security control assessor, performing non-technical and technical assessments on HIGH, MODERATE, and LOW systems. Responsible for Developing the appropriate documentation and reports necessary to validate systems that meet security and privacy requirements in accordance with the Risk Management Framework (RMF) authorization process. Oversee the preparation of comprehensive Certification and Accreditation (C&A) Packages for submission to the Authorizing Officials for approval of an Authorization to Operate (ATO) Security Control Assessor NCR 2018 to December 2018 Responsible for all phases of C&A to ensure

compliance and provide guidance on IT Security requirements assigned to stakeholders. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, NIST 800-53 rev4, FIPS 199, FIPS 200 and OMB A-130 Appendix III, etc. Assess and review Certification and Accreditation (C&A) package in view of clients' quarterly and annual in line with FISMA Acts of 2002. Conducts the ST&E Execution via document examination, interviews and manual assessments. Identify security controls and construct a compliance matrix for tracking Hold kick-off meeting with system owner, ISSO and other stakeholders to discuss assessment activities Perform vulnerability assessment of information systems to detect deficiencies and validate compliance using management tracking tool. (CSAM) Interface with system owners and administrators to present the vulnerability finding and recommendation remediation strategy. Develop plan of actions and milestones for documenting, prioritizing, remediating, monitoring, and corrective actions. Participate in POA&M review closure Perform Security Categorization (FIPS 199), conduct assessment and review Privacy Threshold Analysis (PTA), E-Authentication, Contingency Plan and Testing for compliance and completeness. Perform Examination, Interview, and Testing (EIT) Review and document Security Test & Evaluation (ST&E), Security Assessment Plan (SAP), and Security Assessment Report (SAR). Creating Standard Operating Procedures (SOP) in support of information system. Develop, review, update and document SAR, SSP, CP, and POA&M. Collaborate with other stakeholders to achieve maximum security goals and objectives. Information Security Analyst OKINYX IT, MD July 2014 to February 2017 Develop, review, and update Information Security System Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, NIST 800-53 rev4, FIPS 199, FIPS 200 and OMB A-130 Appendix III, etc. Performed Federal Information Security Management Act (FISMA) audit reviews using NIST 800-37 rev 1. Updated IT security policies, procedures, standards, and guidelines according to private and federal requirements. Performed risk assessments, developed and review System Security Plans (SSP), Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration

Management Plan (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation in accordance with NIST SP 800-37 rev 1, 800-18, 800-53 rev 4 and 800-34. Performed vulnerability and baseline scans on the client network using Retina Network Security Scanner (RNSS) and Nessus in accordance with the organization Continuous Monitoring Plan and NIST 800-137. Analyzed security reports for security vulnerabilities. Worked with IT Operations and Network Engineers to mitigate system vulnerabilities discovered in network devices (routers, switches, VPN Concentrator), servers, and workstations. Familiar with NIST Publications SP 800-18, SP 800-30, SP 800-37 rev 1, SP 800-53 rev 4, SP 800-53A, SP 800-60 and Federal Information Processing Standards (FIPS) - FIPS 199 and FIPS 200. Provided day-to-day customer support for all aspects of the cloud computing platform via telephone, email, and ticketing/monitoring system. Prioritized and managed service requests, incident management, escalation, and reporting to maintain service level agreement. Monitored the status of the cloud computing platform using operations monitoring tools and procedures. Working knowledge of duties required to implement information security controls and lead information security initiatives. Ability to translate business requirements into control objectives. IT Security Specialist Midland Financial Services November 2012 to July 2014 Conducted security assessment on information systems. Reviewed systems for adequate management controls, efficiency and compliance with policies and regulations. Made recommendations when necessary. Conduct Information System Audit ( Security Control Assessment) and Security Authorization. Performed risk assessments, developed and review System Security Plans (SSP), Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plan (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation in accordance with NIST SP 800-37 rev 1, 800-18, 800-53 rev 4 and 800-34. Analyzed vulnerability scan results and conduct risk assessment of findings from the information system assessment. Responsible for auditing POA&M closures to ensure that identified weaknesses/vulnerabilities are remediated as scheduled and the information system's security requirements are satisfied. Planned and performed review of IT general and Application controls. Identify and communicate security

findings to senior management. Conducted annual review of security policies and procedures. Maintained a good working relationship to enhance customer satisfaction. Ensured timely follow up on management action plan for completed assessment and reports quarterly remediation status to the management. Information Technology Specialist NAMA March 2008 to June 2012 Research and resolve technical issues, maintain technical aptitude and support corporate initiatives and team department goals according to direction of management. Worked closely with clients and staffs to ensure smooth, uninterrupted operation of network client workstations, servers, and all related peripherals. Perform scheduled software and hardware installations to workstations. Performed data backups and disaster recovery operations. Maintained and administered computer network and related computing environments. Including computer hardware, system software, applications software and all configurations. Performed routine network startup and shutdowns procedures, and maintained control records. Develop help sheets and knowledge base articles for end users. Identify and learn appropriate software and hardware used and supported by the organization. Ensured that all production changes are processed according to Change Management policies and procedures. Updated the Change log with all progress that occurred. Understood and analyzed Business, Technical, Functional and User Interface requirement of a project. HelpDesk Support NAMA August 2006 to March 2008 Provide first point of contact for support issues. Interact with users to provide and process information in response to problems, inquiries, concerns and/or requests. Collaborate with customers to resolve application, phone, printer, or computer problems in real time. Provided in-depth and high level technical support to the General Counsel of the Nigerian Airspace Management Agency on hardware, software, and network related problems, questions, and use. Troubleshot, resolved, integrated, tested, and maintained operating systems environments such as, but not limited to: Windows 7, MS Office, etc. Interviewed user to collect information about problem and leads user through diagnostic procedures to determine source of error; determines whether problem is caused by hardware such as modem, printer, or cables. Managed users, security groups, and computers through Active Directory. 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. Supported users having data and network connectivity issue. Monitored network performance and troubleshoot problem areas as needed. Provided first level support to customers before escalation. Installed, configured and troubleshoot software. Cross-trained and provided back-up for other IT support representatives when needed. Displayed exceptional telephone etiquette and professionalism in answering and resolving technical call. Account Auditor NAMA March 2003 to August 2006 Responsible for accounting services including accounts payable, preparation of payroll checks, maintaining records on inventory/fixed assets and other accounting activities for NAMA. Monitored accounting records to ensure accuracy and integrity of accounting records. Ensures compliance with established internal control procedures by examining records, reports, operating practices, and documentation. Verifies assets and liabilities by comparing items to documentation. Inspect account books and accounting systems for efficiency, effectiveness, and use of accepted accounting procedures to record transactions. Collect and analyze data to detect deficient controls, duplicated effort, extravagance, fraud, or non-compliance with laws, regulations, and management policies. Prepare detailed reports on audit findings and communicates the findings report to management. Maintains professional and technical knowledge by attending educational workshops; reviewing professional publications; establishing personal networks; participating in professional societies. Contributes to team effort by accomplishing related results as needed. Education B.Sc. in Information Security Lagos State University - Lagos, NG Skills Security, Cobit, Information security, Itil, Nessus, Nist, Fisma, Federal information security management act, Document management, Configuration management, Document management systems, Assurance analyst, Information assurance, Content management, Documentation, Auditing, Ecms, Internal controls, Best practices, Scanning Additional Information Skills Demonstrated experience as a Security Analyst or Information Assurance Analyst Vast knowledge of IT Service Management (ITSM) based on ITIL best practices. Specialize in ITIL Service Support areas of Incident, Problem, Change, Release, Configuration Management and Service Desk. Ability to evaluate the adequacy and effectiveness of Client's internal controls using

risk-based methodology developed from professional auditing standards such as COBIT and FISCAM. Specialize in the Federal Information Security Management Act (FISMA) and the Security Authorization process based on NIST RMF 800-37 Rev.1 Coordinate in-depth interviews and examine documentation and artifacts in accordance with NIST SP 800-53A and 800-53 rev 4 Proven ability to thrive in a team environment but capable of operating independently Conversant with security-scanning tools such as Nessus, WebInspect , AppDetective and Retina Proficient in the use of Document Management Systems such as Enterprise Content Management Software (ECMS) and Trusted Agent FISMA (TAF).

Name: Zachary Gregory

Email: xspence@example.com

Phone: 001-932-460-1516