Cyber Security Analyst/ IT Auditor Cyber Security Analyst/ IT Auditor Cyber Security Analyst/ IT Auditor - PotomacWave Consulting New York, NY Work Experience Cyber Security Analyst/ IT Auditor PotomacWave Consulting December 2016 to Present Implement step-by-step guidance for client's high risk control to assist in remediating findings . Update risk score baselines to measure remediation over time and help prioritize client's cybersecurity projects Support client in implementing a Data Loss Protection program Coordinate meetings and tasking with system owners and support remediation of open items Assist in ensuring that vulnerabilities identified in client's IT security POA&M database are addressed promptly by working with system owners and managers Assist with creating strategies to achieve cyber-related objectives including due dates, critical paths, and milestones to exceed project goals Assess the information technology systems, security regulatory risk management and security vulnerabilities; using the NIST SP 800-series and FIPS Conduct security control assessments and control test of design and operating effectiveness to ensure adherence to customer specific security policy, procedures and industry standards Schedule, track and manage quarterly Plan of Action & Milestones (POA&M) review process Monitor, evaluate, and assist with the maintenance of assigned security systems and assist with the review and definition of security requirements Analyze and evaluate complex business and technology risks, internal controls and related opportunities for internal control improvement Collaborate with clients and the system development teams to design and implement controls to appropriately secure the data at rest, in use and in motion Build and nurture positive working relationships with clients with the intention to exceed client expectations Comply with security systems and respond to internal and external customer request for computer security information and reports Provide support for system reviews to determine if they are designed to comply with established standards Facilitate use of technology-based tools or methodologies to review, design and/or implement products and services IT Auditor/ Cyber Security Analyst Tantus Technologies January 2016 to December 2016 Conducted several Security Controls Assessments (SCAs) from the planning phase through to client follow-up for several systems Assessed design and operating effectiveness of IT Controls for several information system boundaries using

corresponding System Security Plans (SSP), according to the National Institute of Standards and Technology (NIST) 800-53 publications Performed Federal Information System Management Act (FISMA) compliance audits Identified control gaps and created Plan Of Action & Milestones (POA&Ms) reports for vulnerable systems Assisted in the development of appropriate information security policies, standards, procedures, checklists, and guidelines using generally-recognized security concepts tailored to meet the requirements of the organization Identified document, and assessed information security vulnerabilities and risks in the information technology environment Evaluated identified vulnerabilities and risks, working with business owners, risk management, and IT leaders Identified tasks and controls necessary to remediate identified risks and vulnerabilities; negotiated dates for remediation to be complete Prepared and updated comprehensive Assessment & Accreditation (A&A) packages Tracked progress on remediation of identified risks and vulnerabilities and provide appropriate reporting to constituents Conducted Security Impact Analyses (SIAs) on changes that required them Monitored commercial, Personal, politically exposed persons and money service business accounts for potential suspicious activity including money laundering, organized crime, drug trafficking and terrorism. Conducted internal fraud investigations of customers' account statements, cash, checks, ACH, and wire transfers by reviewing client transaction flow of payments for suspicious activity. Identified red flag issues and escalated within the AML framework for further investigation. Drafted Pre-SAR narratives providing concise statements to assist AML officer with SAR filing. Conducted EDD research via LexisNexis, Google, RDC, and Mainframe Managed the creation of manual & Automated alerts due to possible unusual activity escalated by other departments. Government Contractor Department of Commerce/ Department of Treasury 1st Choice LLC June 2015 to December 2015 IT Auditor/ Cyber Security Analyst *An Information Security professional with diversified experience encompassing Compliance and Risk Management Framework (RMF), Information Security and Assurance, System Development Life Cycle (SDLC), Security Control Assessment, Vulnerability and POA&M Management using different industrial standard frameworks such as OMB, FISMA, FedRAMP, HIPAA, PCI DSS, FIPS 199/200 and NIST 800 SPs (18, 30, 37rev1, 53/53Arev4). A proven project

and team lead with the ability to provide information security support for federal information systems. * Experience in the development of ATO Packages such as System Security Plans (SSP), SAR and POAM. * Able to create and review security artifacts such as System Security Plans (SSP), Contingency Plans (CP), Incident Response Plans (IRP)/Testing, and Configuration Management Plans (CMP), Privacy Impact Assessments and SOPs * Understanding of Cloud protections as expressed in FedRAMP for Federal Government agencies. * Able to develop and implement Technology Controls and Information Security related policies, programs and tools. * Experience documenting technical issues identified during security assessments and recommending improvements in the existing service support tools and "standard findings" * Familiar with network and information system security principles, technologies, and test practices as well as supporting security authorization activities. * Proficient in explaining technical information, resolutions, documentations, and presentations to clients and non-technical personnel at all levels of the organization or enterprise. Cyber Security Analyst / IT Auditor International Development Institute June 2011 to May 2014 Communicated results of audits and reviews to management and work with management to develop remediation plans Reviewed deficiencies and formulated solutions for implementation Planned, performed and documented results of internal audits and reviews Recommended improvements to internal controls to ensure/enhance compliance with company policies. Provided front-line support for all information security related issues, such as firewall configuration, advising on security policy compliance, handling data confidentiality issues, monitoring and responding to emerging threats, and security compliance projects (e.g. FISMA). Reviewed results of Nessus vulnerability scans to ensure the systems are devoid of critical and high vulnerabilities. Worked with appropriate system managers and operations personnel to remediate identified vulnerabilities. Followed up with management to confirm remediation plans are completed as scheduled Assisted Managing Directors, Senior Managers and Managers with various initiatives related to business development and practice development Reviewed junior staff's progress to ensure compliance with audit program and professional standards. Reviewed timelines and budget to ensure compliance with customer needs Proactive mitigation of network

and operating systems vulnerabilities and recommending compensating control Supported and conducted the examination of transactions across regions linking up pockets of suspicious activity and/or intelligence to provide a consolidated view of FCC issues. Prepared Suspicious Activity Reports (SARs) and prepared for filing. Interact with Senior Management on the Compliance, Legal and business sectors concerning AML issues. Knowledgeable of the laws applicable to money laundering, including the Bank Secrecy Act, the USA PATRIOT act, US Treasury AML guidelines, OFAC requirements, and Suspicious Activity Reporting requirements. In conjunction with Core Teams, responsible for the full range of AML program activities (policy, risk assessment, testing, transaction monitoring, suspect screening operation, OFAC compliance, business process analysis, program execution, and outreach and liaison activities). Provided AML advice to the business based on regulatory requirements, firm policies, standards, regulatory mandates and commitments. Reviewed and filed currency transaction reports (CTRs). United States Congresswoman Gwen Moore /SUNY Capitol Hill Fellow Washington, DC, Jackson & Hewitt Tax Consultants IT Audit Intern Strategic Human Capital - New York, NY January 2011 to May 2011 team in the Office of Human Resource Management. Assessed current state vs. future state processes and programs; made recommendations to optimize human performance. Presented recommendations to senior leadership teams to direct strategic organizational development. Supported strategic human capital investment efforts by editing a strategic alignment matrix using Microsoft excel and PowerPoint to demonstrate how VA strategic plan corresponds with service level goals and objectives. Applied research methodologies and consultative expertise to develop data-driven assessments; presented recommendations to senior leadership teams in efforts to direct federal human capital strategy, virtual training and program design Administrative duties such as scheduling meetings, organizing client services and office management Conducted research and collected statistics for Congresswoman in relation to her constituent projects Monthly reports including EEO/diversity, attrition, and ad-hoc reports Competency-based job descriptions and performance evaluations for current and future interns, in consultation chief of staff. Jackson & Hewitt Tax Consultants IT Audit Intern, New York, January 2008- January 2011 Performed audit

planning, conducted walkthroughs, and assessed the internal control environment through control testing Ensured that policies and procedures were implemented and well documented Performed internal reviews and identified compliance problems that called for formal attention. Provided day-to-day execution of audit engagements and projects such as SOX, compliance audit, and operational audit Performed Information Technology audits (e.g. information security, change management, computer operations) for clients from various industries (manufacturing, technology, education, healthcare, etc.) Documented clients' internal controls (both IT controls and some business cycle controls) Prepared work papers supporting audit results Prepared audit reports detailing results of audits and provided written recommendations to clients based on results Liaised with external auditors for remediation of findings Performed Tests of Design (TODs), Tests of Effectiveness (TOEs) of Key defined control activities and tested for Audit Readiness Education Master's in Cybersecurity & Information Assurance Western Governors University January 2017 to Present Masters in HR Information Systems Georgetown University B. A. In Political Science and Economics Minor Law in Political Science and Economics Minor Law SUNY Old Westbury - Old Westbury, NY Skills Siem, Information Security, Nist, Cyber Security, Cissp, It Audit, Cobit, SOX, Cisa, Fisma

Name: Larry Liu

Email: dsanchez@example.com

Phone: 830-250-0120