IT Audit Analyst IT Audit Analyst IT Audit Analyst - Nationwide IT Services Washington, DC Visionary, dynamic, results-driven, and analytical Cyber Security professional, equipped with over 5+ years of hands-on experience, cutting edge knowledge, state-of-the-art multi-technology in both federal and commercial sectors. Experienced in performing security assessments of client IT environments against various industry standards and regulations including PCI, HITRUST, ISO 27001/2, HIPAA, and Sarbanes-Oxley. Work Experience IT Audit Analyst Nationwide IT Services - Washington, DC June 2018 to Present Reports to the Senior Program Manager, and functions as part of the IT Audit Team responsible for conducting security audits, and providing oversight and leadership for tasks and deliverables, ensuring the timely and successful completion thereof in accordance with a project management plan, and presenting findings and solutions to the client in a clear and concise manner. ? Interfaces with clients to review and analyze complex systems (Applications, operating systems, databases, and Networking devices), to identify risks, exposures, define and implement compensating controls ? Works independently to collect, consolidate and analyze information required for the evaluation of security controls and gaps ? Produces final reports on compliance to detail the controls observed during security assessments in accordance with various security standards and regulations (PCI, HITRUST, ISO 27001/2, HIPAA, Sarbanes-Oxley, etc.) ? Provides guidance to prepare organizations for Statement on Standards for Attestation Engagements No. 16 (SSAE 16) audits ? Manages client's third-party assessment program, including security assessments, task tracking, analyses reporting, documentation and process improvement. ? Completes tests on financial system controls compliance (OMB A-123), IT General Computer Control (ITGC), and Application Controls ? Utilizes audit procedures (Testing, Interviewing, and Examination) to determine the design and operating effectiveness of the controls ? Develops and writes reports and Corrective Action Plans (CAP) identifying findings and providing recommendations ? Performs walkthrough interviews and maintains communication with a variety of client stakeholders, including system personnel such as system and database administrators ? Requests, obtains, reviews, and analyzes a variety of artifacts to assist in executing IT controls testing such as Security Plans, SOPs, system screenshots, and system configuration settings

Security Analyst DIGITAL GLOBAL CONNETED - Washington, DC April 2013 to May 2018 Reported to the Information System Security Manager (ISSM) and was responsible for guiding system owners and their teams through the ATO process using the NIST Risk Management Framework (RMF). ? Collected systems information (information type, boundary, inventory, etc.) and assisted with categorizing systems based on NIST SP 800-60. ? Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M). ? Assisted with the development of system security plans to provide an overview of federal information system security requirements and described the controls in place or to meet those requirements. ? Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk assessments (RAs), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs). ? Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. ? Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. ? Conducted IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. ? Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. ? Assisted the ISSM with Plan of Actions & Milestone (POA&M) updates, maintenance, and coordination with the SCA. Perform Security Briefings for personnel on Rules, Responsibilities, and Acceptable Use Compliance Analyst First Impression Staffing - Washington, DC August 2012 to April 2013 Reported to the Chief Compliance Analyst, was primarily responsible for applying knowledge of Cybersecurity and privacy analysis and consulting to the security assessment and compliance life cycle process. Under the Office of the Chief Information Security

Officer (CISO's) team approach to auditing, participated in IT audits, inspections, and evaluations of the Board's mainframe and distributed computer processing environments. ? Ensured that security policies, procedures and recommendations complied with OFAC, BSA and Organizational guidelines and technical best practices. ? Established system security documentation; assisted with the implementation of security procedures; and verified information system security requirements; ? Provided support for organization's risk management, policy, and technical governance processes to facilitate compliance with applicable laws, regulations ? Initiated compliance and vulnerability scan request to identify and report weaknesses and potential security breaches. ? Executed testing of controls to assess operational effectiveness in managing risks. ? Communicated information to management through presentations and audit reporting. ? Managed remediation of audit findings and maintained understanding of applicable regulatory and compliance requirements ? Ensured timely completion of assigned project phases. Conducted security assessment on information systems. Reviewed systems for adequate management controls, efficiency and compliance with policies, regulations and accounting principles. Principal Audit Assistant Accra Technical University August 2010 to March 2012 Attended opening meetings and documented system notes for use during an audit review ? Conducted risk assessments of assigned department or functional area in a required timeline ? Established risk-based audit programs ? Reviewed the suitability of internal control design ? Conducted audit testing of specified area and identified reportable issues and dimension of risk ? Determined compliance with policies and procedures. ? Verbally communicated findings to senior management and draft comprehensive and complete report of audit area in exit meeting. ? Undertook follow-up reviews and monitored outstanding management actions from previous audits. ? Discussed audit findings and recommendations with senior management and drafting audit reports for review Education BSc in Business Administration Garden City University College Skills Security, Backups, Hipaa, Iso, Iso 27000, Nist, Pci, Sox, Fisma, Network security, Change management, Configuration management, Deployment, Risk analysis, Software development, Information assurance, Contingency planning, Maintenance, Telecommunications, Logging, It Audit, Auditing Additional Information Functional Skills ? In-depth knowledge and experience with ISO 27000 series, PCI DSS, HIPAA, SOX and risk analysis methodologies and security standards ? In-depth knowledge and experience in IT Security and Telecommunications, including access controls, network Security, logging/monitoring, vulnerability assessments, system hardening, and secure software development ? Advanced level experience in testing and remediating: Configuration management, including configuration baseline concepts, baseline deviations, baseline maintenance, monitoring for ongoing compliance with a baseline, and industry-accepted baselines such as DISA STIGs and CIS benchmarks, change management, including authorization, development, testing, and deployment of changes, and Contingency planning, including backups, testing of backups, and alternate sites ? Extensive working knowledge of FISMA, NIST SP 800 series, FISCAM, and other relevant federal information assurance laws, regulations, and guidance. ? Experience performing OMB Circular A-123 or similar internal control assessments

Name: Daniel Murray

Email: dmartinez@example.org

Phone: 228.439.9299