IT Security Analyst IT Security Analyst IT Security Analyst - Maximus Federal Woodbridge, VA Seeking an IT Security Auditor or Cyber Security Analyst in a growing organization with focus on FISMA, Sarbanes-Oxley 404, HIPAA, PCI DSS, HITRUST, Vendor Risk, System Security Monitoring, Risk Assessments or other information system security programs. Authorized to work in the US for any employer Work Experience IT Security Analyst Maximus Federal - Washington, DC January 2018 to Present Responsible for conducting structured security certification and accreditation (C&A) activities utilizing the Risk Management Framework and in compliance with the Federal Information Security Modernization Act (FISMA) requirements Conduct Business Impact Analysis (BIA) to analyze mission-critical business functions, and identify and quantify the impact those functions if these are interrupted Conduct IT system testing based on the appropriate analysis and review techniques provided by NIST Develop and update the information systems security documentation (e.g., System Security Plan, Contingency Plan, Contingency Plan Test, Business Impact Analysis, FIPS-199, eAuthentication, Privacy Threshold Analysis, Privacy Impact Assessment, System of Records Notice) Experience using NIST SP 800 series including SP 800-60, SP 800-53, SP 800-53A, SP 800-18, SP 800-34, SP 800-62, SP 800-37, SP 800-137 Assess adequacy and efficiency of security controls by updating Security Control Assessment Plan (SCAP), Security Test & Evaluation (ST&E) Report and Security Assessment Report (SAR) Plan, execute and report on IT system vulnerability root causes and mitigation recommendations Provide a security review of system documentation, audit logs, rule set and configuration to validate policy compliance. Report IT security incidents in accordance with established procedures Plan, develop, implement, and maintain an Incident Response and Audit Program for events of interest and address Plan of Action and Milestones (POA&Ms) in continuous monitoring with various point of contact Plan, schedule, coordinate, prepare, execute, document the results of test plans and test scripts, and provide lessons learned for incident response, contingency, and continuity of operations drills, exercises, and activities. Effectively communicate technical information to non-technical personnel via email, face-to-face meetings and periodic bulletins Coordinate with system owners and ISSOs across the organization to ensure timely compliance Participate in meetings to discuss system boundaries for new or updated systems to help determine information types for categorization purposes. Determine the classification of information systems to aid in selecting appropriate controls for protecting the system. Information Security Analyst Forever Solutions Group - Frederick, MD August 2016 to December 2017 Participate in meetings to discuss system boundaries for new or updated systems to help determine information types for categorization purposes. Determine the classification of information systems to aid in selecting appropriate controls for protecting the system. Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M). Assist System Owners and ISSO in preparing certification and Accreditation package for IT systems, to ensure management, operational and technical security controls are adhering to. Utilizing NIST SP 800-53 Revision 4 and NIST SP 800-53A Revision 4 in conducting security control assessments. Perform Vulnerability Assessment. making sure that risks are assessed, evaluated and a proper action have been taken to limit their impact on the information and information systems. Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Create reports detailing identified vulnerabilities and the steps to remediate them Update IT security policies, procedures, standards, and guidelines according to SP 800-53 Rev 4. Designing, developing and implementing solutions to IT security requirements at various levels of the agency's System Development Life Cycle (SDLC) through the Program Manager. Participating in change control board meeting to ensure changes to systems are evaluated, tested and approved before promoting into production environment. IT Compliance and Risk Analyst Dun & Bradstreet - Short Hills, NJ December 2014 to August 2016 Conduct kick-off, entrance and exit meetings among IT team and system owners respectively in a diligent manner to gather needed information/evidence and address issues identified. Liaise with Application owners to perform walkthroughs and testing of IT general controls, automated and IT Dependent manual controls for applications supporting financially significant systems and processes. Perform tests on IT Infrastructure to ensure that access levels are appropriate and software updates have been installed. Liaise with external auditors during the test of IT applications and systems as part of the annual financial statement audit. Prepare all the information requested on their client request list as it relates to my area of work and provide any needed support. Develop Test plan, define control description and control statements. Schedule interview and walkthrough meetings with Business and Application Owners. Coordinate with Application and other stakeholders to gather evidence. Review control evidence to ensure they are complete and adequate. Identify control weakness and communicate with management the recommended remedies for the identified risks and vulnerabilities. Prepare concise and professional reports on the audit projects for presentation to management and for future reference in regards to subsequent audit assignments. Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard [PCI DSS] Updated Business Impact Assessment [BIA] template to monitor efficiency and adequacy of Contingency plan. Plan, schedule, coordinate, prepare, execute, document the results of test plans and test scripts, and provide lessons learned for incident response, contingency, and on-going monitoring activity. IT Risk Analyst PwC - Accra, GH November 2011 to December 2014 Ghana. Participated in audits of general controls and automated business controls of consumer banking and mortgage technologies and back office processing. Assisted with the planning and scoping of audits, including performance of walk-throughs and preparation of work programs. Developed integrated audits using risk-based assessments of systems and performed general control reviews of consumer banking and mortgage technologies and back office processing. Participated in reviews of risk management, data governance, vendor management, systems processing, and network and database security and recovery controls. Assisted in the interpretation and communication of information to management. Wrote audit work papers and reports with minimal intervention by the Audit manager. Education Bachelor of Science in Accounting in Accounting University of Professional Studies - Accra, GH Skills SECURITY (3 years), SHAREPOINT, NIST (2 years), PCI (1 year), FISMA (Less than 1 year) Additional Information

AREAS OF EXPERTISE FISMA, NIST SP 800 Series, COSO, COBIT, Sarbanes-Oxley Act, HIPAA, HITRUST, PCI DSS, ISO 27001, 27002, Security Assessment & Authorization (SA&A), FIPS, Strong verbal and written communication. SOFTWARE AND PLATFORM Windows, Microsoft Word, Excel, Access, Outlook, Power Point, SharePoint, VBA/Macros, VMWare, Tableau, Crystal Reports, Qualtrics, CSAM, TAF, Xacta, GRC SUMMARY OF QUALIFICATIONS A confident, goal-oriented and versatile IT Audit professional, with a wide-range of experience and profound knowledge in industry IT control frameworks and standards. A proven track record with over 5 years of direct hands-on experience in IT auditing with emphasis on delivering security solutions to meet business objectives while reducing operational risk. My expertise includes NIST Risk Management Framework (RMF), Information Assurance, System Monitoring, regulatory compliance and loss mitigation. Supporting client on FISMA compliance- [categorization through to continuous monitoring] and other commercial frameworks including COSO, COBIT, ISO 27001/27002, SOC Reports, SSAE 16, HITRUST, HIPAA and Vendor (Third and Fourth Party) Risk Assessment.Professionally composed and organized individual with well-developed communication skills demonstrated through extensive multicultural perspective and positive interaction

Name: Michael Park

Email: carla07@example.net

Phone: (771)347-5758