IT Security Analyst IT Security Analyst IT Security Analyst - Top Group Technologies, Inc Hanover, MD Work Experience IT Security Analyst Top Group Technologies, Inc - Waldorf, MD April 2017 to Present Federal Contractor Conduct kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Conduct IT controls risk assessments including reviewing organizational polices standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Assist with the development of system Security Plan (SSP) to provide an overview of federal information system security requirements and described the controls in place to meet those requirements. Conduct document reviews of NIST, OMB, FISMA and other policy documents and vendor publications related to enterprise technologies and recognize, modify and update procedures resulting from the new guidance. Develop Security Assessment Reports (SAR) detailing the results of the assessment along with Plan of Action and Milestones (POA&M). Provide Continuous Monitoring support through POA&M's, system and user audits, analyze and report scanning results, and update all corresponding security documents as needed. Provide senior level security consulting to Federal customers in addition to guidance and support to Department ISSOs/System Owners on the FISMA and NIST Security Assessment and Authorization process. Prepare Security Assessment and Authorization (SA&S) packages to ensure management, operational and technical security controls adhere to NIST SP 800-53 standards. Assist System Owners and ISSO in preparing certification and Accreditation package for company's IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4. Provide ISSO and CISO support by assisting in reviewing risk waivers and ISA, MOU review before authorization. Create and update the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, System Security Plan (SSP), Risk Assessment (RA), Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, System Security test and Evaluation (ST&E), Contingency Plan, Plan of Actions and Milestones (POA&M). IT Security Analyst Dynamics Technologies Solutions - Largo, MD July 2014 to March 2017 Developed security control test plans and conducted in-depth security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and polices safeguards to maintain NIST compliance. Updated System Security Plan, Risk Assessment, Privacy Impact Analysis, ST&E and POA&M. Conducted Information systems security risk assessments including reviewing organizational polices standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Conducted comprehensive assessment of the management, operational, technical security control employed within or inherited by an Information System to determine the overall effectiveness of the control. 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. Reviewed security policy documents and make recommendations on documentation compliant. Created and updated the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, SSP, RA, E-Authentication, ST&E, Contingency Plan, and (POA&M). Assisted System Owner and ISSO in preparing certification and Accreditation package for major systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4. Performed vulnerability assessment, making sure risks are assessed and proper actions taken to mitigate them. Database Administrator Pyramid Solutions - Vienna, VA February 2013 to June 2014 Implemented and maintained database systems. Performed routine backups, including use of Oracles datapump export and RMAN utilities. Applied security patches and bug fixes. Assisted developers in performance and tuning queries and SQL. Monitored database performance and recommended and implemented changes to achieve higher performance. Performed daily checks on database servers, confirming status of backups, file compression, and exports; troubleshoot any errors. Education MBA University of Maryland - Adelphi, MD July 2019 Bachelors in Business Administration University of Lagos - Lagos, NG October 2000 compliance NIST Skills Security, Share point, Nessus, Remedy, Peoplesoft

Name: Nicholas Carson

Email: doughertygregory@example.com

Phone: (296)486-6421x88345