Information Security Analyst Information Security Analyst Information Security Analyst - KPMG New Carrollton, MD Specializes in National Institute of Standards and Technology (NIST)/ Federal Information Security Management Act (FISMA) Compliance, IT Auditing, Risk Management, Business Continuity and Security Policy. Extensive background and experience in information security, IT infrastructure, and maintenance of large information systems. Hands-on experience in vulnerability assessment, implementation of the Plans of Actions and Milestones/ Corrective Action Plans, as well as remediation of the documented threats and vulnerabilities. Very knowledgeable of industry standards and proven track record of implementing the necessary controls to ensure compliance. Commitment to maintaining a reputation built on quality, service and uncompromising ethics. Authorized to work in the US for any employer Work Experience Information Security Analyst KPMG - Washington, DC November 2015 to Present Experience in Categorizing systems using FIPS 199 and NIST SP 800-60 Assist Systems Owners and ISSO in preparing certification and accreditation packages. Experience in testing management, operational and technical security controls. Perform vulnerability assessment. Make sure that risks are assessed, evaluated and proper actions have been taken to limit their impact on the information and information systems. 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 Action and Milestones (POA&M) Conduct Self-Annual Assessment (NIST SP 800-53A) 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 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. Security Analyst Deloitte - Washington, DC June 2014 to October 2015 * Conducted IT Risk Assessment and documented key controls * Assessed System Security Controls using SP 800-53A. * Adhere to client security standards and industry best practices. * Develop, review and evaluate Security Plan based on NIST Special Publications 800-18 * Investigates possible security breaches identified through review of audit reports and follow up accordingly with departments/ management * Maintained and developed expertise with all current, and future, organizational policies and procedures relating to information technology * Performed risk assessment s to ensure organization data remains protected by assessing departments and individuals on their data integrity and reporting and acting on any issues. * Developed test plans, testing procedures and documented test results and exceptions * Assist with development of security standards and procedures. * Assess information assurance controls for compliance * Evaluate, test, recommend, coordinate, monitor and maintain information assurance controls * Creates and/or recommends a system for updating training materials, monitoring training progress, and documenting completed training. IT Security Analyst System High Corporation - Chantilly, VA January 2011 to June 2014 * Conduct IT risk assessment to identify system threats * Conducted security control assessments to assess the adequacy of management, operation privacy, and technical security controls implemented * Business Impact analysis (BIA) to analyze mission-critical business functions, and identify and quantify the impact if these are lost (e.g. operational, financial). BIA helped to define the company's business continuity plan and IT internal control audit objective. * Provided expertise on technical services including all aspects of information security * Assessed system design and security posture as well as advising information security compliance with FISMA and NIST SP 800-53 controls. * Conducted forensic traffic logs analysis to isolate issues and respond to analyst alerts * Performed maintenance and advanced configuration of systems in order to protect systems from emerging cyber threats. Education M.S. in Cyber Security Management and Policy University of Maryland University College May 2020 B.S. in Kinesiology University of Maryland December 2008 Skills Security, Business continuity, Iso, Iso 27001, Nist, Pci, Sox, Fisma, It auditing, Auditing

Name: Jason Martin

Email: vdelgado@example.net

Phone: (507)400-0979