Information Security Analyst Information Security Analyst Information Security Analyst - Cloud Security Elkridge, MD Work Experience Information Security Analyst Cloud Security January 2014 to Present TEKsystems ? Ensure implementation of appropriate security control for Information System based on NIST Special Publication 800-53 rev 4, FIPS 200, and System Categorization using NIST 800-60, and FIPS 199. ? Conduct CDM meeting to discuss vulnerabilities and potential remediation actions with system and application owners. ? Ensure identified weaknesses from vulnerabilities scans are remediated in accordance with defined time frames ? Play a leading role in designing and integrating marketplace leading vulnerability management, threat management, monitoring, and data protection processes and platform tools ? Experience in developing test plan for assessment and documenting security controls across variety of systems. ? Involved in Amazon Web Services technology, AWS security offerings, experience with AWS: VPCs, IAM, Security Groups, EC2, EBS, etc. Perform Cloud security evaluations for A&A and Continuous Monitoring processes, Explain cloud security controls, requirements, guidance and Identify cloud architecture best practices. ? Involve in security awareness program to educate employees and managers on current threat and vulnerabilities ? Working knowledge in deployment pipelines, and automated build and configuration tools ? Involved in identifying security gaps and providing security recommendation to address gaps and complete risk profile ? Conduct security control assessment to assess the adequacy of management, operational privacy, and technical security controls implemented ? Develop Security Assessment Report (SAR) detailing the results of the assessment along with Plan of Action and Milestones (POA&M) ? Conduct follow up meetings to assist information system owners to close/remediate POA&M items ? Develop System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements ? Conduct IT risk assessment to identify system threats, vulnerabilities, and risks ? Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. ? Worked with system application team conducting interviews and collecting artifacts relevant to the assessment of security controls ? Worked on application development specifically developing multi-tiered application, Service-Oriented Architecture (SOA) web-based application and distribute enterprise applications. IT Security Analyst IPNS May 2013 to December 2013 Developed a security baseline controls and test plan that was used to assess implemented security controls ? 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) ? Responsible for auditing the security framework for existing and new enterprise technologies. ? Ensured successful implementation and maintenance of defined security standards. ? Responsible for information gathering, analysis, and incident response associated with enterprise technologies. ? Provided technical support for the enhancement of, and changes to security infrastructure configurations. ? Analyzed data related to security incidents and monitored compliance. IT Security Analyst Enlightened Inc June 2012 to May 2013 Developed and conducted ST&E (Security Test and Evaluation) according to NIST SP 800-53A. ? Applied current computer science technologies and Information Assurance (IA) requirements to the analysis, design, development, evaluation, and integration of computer/communication ? systems and networks to maintain an acceptable system security posture throughout the lifecycle of multiple national level mission system. ? Developed, maintained, and communicated a consolidated risk management activities and deliverables calendar. ? Conducted meetings with the IT team to gather documentation and evidence about their control environment. ? Worked with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans. ? Performed comprehensive Security Control Assessment and write reviews for management, operational and technical security controls for audited applications and information systems. Education Bachelor of Science degree in Computer Information Systems University of Cape Coast 1990 to 1994 Additional Information A dynamic and detail-oriented Security Assessment and Authorization professional with strong problem solving and project management skills knowledgeable in Risk Management Framework (RMF), Systems Development Life Cycle (SDLC), Security Life Cycle and Vulnerability Management, using FISMA and applicable NIST standards. Experienced with Cloud Security requirements, processes, and procedures needed to secure the cloud environment and AWS Well Architected Framework, Best Practices and Services (such as EC2, VPC, S3, Security Groups, IAM, CloudWatch, CloudFormation and CloudTrails), A great team player with the ability to work independently, under pressure and with little or no supervision.

Name: Curtis Adams

Email: brian61@example.org

Phone: 001-594-698-5732x5791