

Information Security Analyst Information Security Analyst Information Security Analyst - SeNet International Inc Olney, MD Seeking a Cyber Security position in a growth-oriented organization with emphasis on FISMA, system security evaluation, validation, monitoring and auditing, risk management, audit engagements, testing information technology controls and Sarbanes-Oxley 404.

Work Experience Information Security Analyst SeNet International Inc - Fairfax, VA October 2013 to Present Provide program support for Health Resource Service Administration (HRSA)'s FISMA Continuous Monitoring initiative and SA&A process.. Determine enterprise risk to HRSA systems and applications and ensure that defined vulnerabilities are mitigated. Perform internal and external security control assessments utilizing Trusted Agent FISMA (TAF) to record assessments data. Develop, track and validate POA&Ms (Plan of Action and Milestone) for assigned HRSA systems and maintain communication with ISSO /System owners on POA&M status and verifies remediation efforts to close POA&Ms. As part of Health Resource Service Administration (HRSA)'s Security compliance team, perform reviews of OMB, NIST, HHS and HRSA policy to modify and update procedures as a result of new guidance. Provide guidance to ISSOs and system administrators on FISMA compliance, and system vulnerabilities. Manage security compliance of assigned systems and maintain all of the FISMA documentations. Analyzes security scans for vulnerabilities and collaborates with ISSOs to remediate findings. Develop Security Control Assessment Plans (SCAP) according to the system categorization, operating environment, and information system functionality and capabilities. Conduct annual security control assessments (NIST 800-53) and documented implementation status and security posture; documented System Security Plans (SSP), Security Assessment Report (SAR), Risk Assessments(RA) and Plans of Action and Milestones (POA&M) for continuous monitoring activities.

Ensure monthly and quarterly vulnerability assessments are conducted for both internal and external system using AppScan and Nessus Ensure change requests adhered to HRSA policy, and CCB reviews requests were processed in a timely manner Conduct kick-off meetings with System Owners and technical team to review SCA Plan, determine the system/application sensitivity and data information. Review and update Awareness training documents, configuration

management Plan (CMP), CP, CPT, SSP, E-Authentication PIA and SOPs for agency. Evaluates and recommends new and emerging security products and technologies IT Security & FISMA Analyst MJHS CORPORATION - Reston, VA August 2009 to September 2013 Assessed program and security controls using Organization IT Security Policy Handbook and NIST Special Publications to provide information necessary to determine their overall effectiveness Developed and maintained C&A documentations, including System Security Plans, Contingency Plans, Risk Assessment Reports and evaluated existing documents and their accuracy Performed Contingency Plan Test and Training to ensure systems' recoverability as defined in IT systems security requirements Involved with creating ST&E documents and helped with reviewing and updating existing ones for several information systems Requested and reviewed vulnerability scans Created POA&Ms and developed mitigation strategies as required Trained and advised IT managers on the FISMA compliance activities and controls Guided System Owners and ISSOs through the Certification and Accreditation (C&A) process so to obtain Authority to operate (ATO) Ensured that management, operational and technical controls for securing either Sensitive Security Systems or IT Systems are in place and are adhered to in accordance to federal guidelines (NIST 800-53) Ensured that appropriate steps are taken to implement information security requirements for IT systems throughout the life cycle i.e., from the requirements definition phase through retirement or disposal. Analyzed user, operational, policy, regulatory, and resource demands and procedures Worked with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans Developed, reviewed and evaluated Security Plan based on NIST Special Publications 800 series Performed comprehensive Security Controls Assessment (SCA) and wrote reviews of management, operational and technical security controls for audited applications and information systems. IT Systems Security Auditor Conducted Information Technology (IT) risk management and assessment Evaluated the design and operation effectiveness of system controls such as access controls, business process controls, data interface controls, key controls and IT general controls Participated and assisted clients to resolve control deficiencies Conducted meetings with the IT team to gather documentation and evidence

about their control environment Developed test plans, test scripts and testing procedures

Documented test results, exception handling process and remediation plans Conducted walkthroughs and documented gaps Performed IT operating effectiveness tests in the areas of security and standard business operations Created change control management process documentation 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 Performed Certification and Accreditation (C&A) documentation in compliance with company standards so as to obtain Authority to Operate (ATO) Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), e-Authentication with business owners and selected stakeholders Developed and conducted ST&E (Security Test and Evaluation) according to NIST SP 800-53A

SAP HCM Consultant XCORDIA TECHNOLOGIES - Columbia, MD June 2007 to April 2009 Industry: Public Sector (Clarks County School District, Nevada.) Facilitated Workshops with SMEs to assess current capabilities and identify high-level business requirements. Created Company Codes, Personnel Areas, Personnel Sub-Areas, Employee Groups and Sub-groups, the Organizational structure to the Hire Process. Participated in User Acceptance Testing (UAT) and assisted in the development of the training manual. Created Business Process Procedures for End Users.

Developed some Deliverables in the Realization Phase:- o The Solution Requirements document, o The End User Training Materials Industry: Oil and Gas 03/2006-04/2007 SAP HCM Consultant

Defined sub-types for HR Master data Created Personnel areas, personnel sub-areas, employee groups and employee subgroups. Enterprise structure comprising of Company Code and Personnel Structure for salaries, hourly exempt and non-exempt. Identify needs for systems development, specify requirements and review data requirements with Development team.

Developed work procedures for user related to SAP system. Validation of end users training and documentation. Developed the following Deliverables: o The Project Charter, the Project plan and the Standards and Procedures. Education Masters of Science in Management University of

Maryland University College - Adelphi, MD March 2012 Bachelor of Science in Accounting Ahmadu

Bello University March 1995

Name: Devin Ortiz

Email: kristopher20@example.net

Phone: +1-232-382-7235x034