Risk & Compliance Analyst Risk & Compliance Analyst Risk & Compliance Analyst - Federal Emergency Management Agency (FEMA) Roswell, GA Authorized to work in the US for any employer Work Experience Risk & Compliance Analyst Federal Emergency Management Agency (FEMA) - Atlanta, GA August 2014 to Present Create remediation strategies for weaknesses based on priorities ? Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards ? Develop and maintain System Security Plans (SSP) and conduct periodic reviews to ensure compliance with the SSP ? Ensure all IS security-related documentation is current and accessible to properly authorized individuals ? Develop and maintain the Plan of Action and Milestones and support remediation activities ? Developing, coordinating, testing and training on Contingency Plans and Incident Response Plans using NIST 800 series ? Perform security control assessment in using NIST 800-53A guidance ? Experience with NIST publications, OMB circulars and memoranda, and FISMA requirements and impact on system security. ? Coordinate with IT System POCs to develop or update the Contingency / Disaster Recovery Plans. Participate in CP/DRP Training and Testing ? Tracks and manages FISMA Assessment & Authorization documentation ensuring required documents and actions are completed within required time schedules ? Supports the ISSO to ensure customer security requirements for IT security are met. IT Security Analyst Federal Emergency Management Agency (FEMA) - Atlanta, GA August 2014 to Present Facilitated and participated in assessments and authorizations (certification & accreditation), compliance reviews, architecture reviews, trainings, plans of action & milestone resolutions, and reports on program status. ? Held kick-off meetings with system owners prior to assessment engagements ? Updated IT security policies, procedures, standards, and guidelines according to private and federal requirements. ? Prepared and submitted Security Assessment Plan (SAP) to ISSO for approval ? Developed and updated system security plan (SSP), plan of action and milestone (POA&M) in CSAM ? Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with NIST standards ? Coordinated with IT System POCs to maintain an accurate

inventory of hardware and software as identified in System Security Plans and Contingency/Disaster Recovery Plans ? Monitors POA&Ms and works with IT System POCs to resolve. Re-assess controls upon POA&M resolution. Provide status reports as necessary ? Prepare and review documentation to include System Security Plans (SSPs), Risk Assessment Reports, Certification and Accreditation (C&A) packages ? Interpreted vulnerability/risk assessment analysis report to support certification and accreditation ? Analyzed system risks and provide recommendations for risk acceptance or rejection ? Develop and/or maintain POA&Ms for all accepted risks upon completion of system SCA, including the utilization of waivers/exceptions where appropriate ? Schedule and conduct security assessments of systems to determine compliance with applicable security controls and standards ? Review security documentation to ensure completeness and accuracy of control documentation ? Compiled and analyzed scan results for weaknesses and vulnerabilities ? Reviewed and revised System Security Plan (SSP), System Security test and Evaluation (ST&E) Risk Assessment (RA), Privacy Impact Assessment (PIA), and the Plan Of Actions and Milestones (POA&M) IT Technical Support Verizon - Ashburn, VA July 2011 to August 2014 Receive and responds to help desk tickets, incoming calls, e-mails, or pages regarding hardware and PC problems ? Handles software and hardware repairs of both laptop and desktop computers ? Resolved PC hardware and software problems ? Escalate support call to supervisor as necessary ? Answer incoming client and customer calls ? Resolved Remedy tickets on a daily basis ? Coordinated with other IT groups for remediation of complex issues Education License in Information Technology American Intercontinental University Additional Information Core Skills ? Performed comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems ? Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and NIST SP 800-53R4 ? Compiled data to complete Residual Risk Report and to insert contents into the POA&M ? Ability to multi-task, work independently and as part of a team ? Strong analytical and quantitative skills ? Effective interpersonal and verbal/written communication skills ? Security Life Cycle and Vulnerability Management, using FISMA and applicable NIST standards. ? Detailed knowledge of

security tools, technologies and best practices with more emphasis on Sarbanes-Oxley 404, COSO, COBIT, PCI-DSS, HIPAA, SAS-70, SSAE 16 and ISO 27001/2. ? Over five years of experience in system security monitoring, auditing and evaluation, C&A and Risk Assessment of GSS (General Support Systems) and MA (Major Applications). ? Performed Certification and Accreditation documentation in compliance with company standards ? Developed, reviewed and evaluated System Security Plan based NIST Special Publications Technical skills Security Technologies: Retina Network Security Scanner, Nessus, Anti-Virus Tools, Web Inspect, Nessus, Systems: Unix-Based Systems, Windows 9X/NT/2000/XP, Networking: LANs, WANs, VPNs, Routers/Switches, Firewalls, TCP/IP Software/Artifacts: MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project, CSAM, FIPS 199, SORN, E-Authentication, PTA, PIA, RA, SSP, CP, CIPT, ST&E, SAR, POA&M, ATO, 800-53A, ISA, MOU, CSAM. Databases: MYSQL, Access, SharePoint, Oracle

Name: Peter Williams

Email: brandon50@example.net

Phone: 923-849-8540x718