IT Security Analyst IT Security Analyst IT Security Analyst - Crest Consulting Group Stafford, VA Work Experience IT Security Analyst Crest Consulting Group August 2012 to Present Conduct meetings with the IT team to gather documentation and evidence about their control environment. Perform Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders. Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A. Apply 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. Develop, maintain, and communicate a consolidated risk management activities and deliverables calendar. Work with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans. Perform comprehensive Security Control Assessment (SCA) and prepare report on management, operational and technical security controls for audited applications and information systems. Review audit logs and provide documentation guidelines to business process owners and management IT Security Analyst Paragon System Inc March 2010 to July 2012 Conducted FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations; conducted out-briefings. Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Miles tones (POA&M), Authorization letter/memorandum (ATO). Assisted with review of policy, security alerts, guidance, regulations and technical advances in IT Security Management Utilized processes within the Security Assessment and Authorization environment such as system security categorization, development of security and contingency plans, security testing and evaluation, system accreditation and continuous monitoring. Contributed to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management. Communicated effectively through written and verbal means to co-workers, subordinates and senior leadership. Item Processor Citi Bank - Washington, DC June 2008 to March 2010 Process routine works in a

prioritized order to meet nightly deadlines for a 30 to 40 million dollar daily operations. Analyze financial performance of various financial centers in the Mid-Atlantic area (44 Financial Centers). Assume leadership role in the absence of management. Identify and resolve all outstanding differences/discrepancies on a daily basis for all Financial Centers. Reconcile financial details and statement with general ledger to complete daily balancing procedures. Communicate with multiple departments within the organization on related issues. Responsible for independently completing accounts payable functions, including analyzing, researching and problem solving. Work with the General Ledger and provide the detail and/or copies of invoices to support the transactions in the GL. Back office teller dealing with daily financial center transaction. Education BS in B/Finance University of Ado, Nigeria - A?? 1999 to 2003 Skills Security Assessment & Authorization, Certification & Accreditation, Security Planning, Vulnerability Scanning, Business Continuity Planning, Risk Assessments, Vulnerability Management, Penetrating testing, PCI (DSS), Security Test & Evaluation, Security Training & Awareness, Incident Response, Policy and Process Development, POA&M Management, MYSQL, MSSQL Server, Access, SharePoint, Oracle, VM ware, Mainframe- RACF, Windows, Unix / Linux, TAF, IDEA, CSAM, XACTA IA Manager, NESSUS, Microsoft SharePoint Additional Information SKILLS SUMMARY: 4+ years of experience in IT Security positions within Commercial and Federal organizations, leading and managing network security, vulnerability management, intrusion detection, help desk, client/customer services. Experienced in NIST, OMB, FISMA and PCI DSS, with various private and federal agencies. Proficient in Security Assessment and Authorization process from initiation to continuous monitoring. Skilled in the development of security plans (SP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, Configuration Management Plans, System Security Checklists, Privacy Impact Assessments, POA&M, Authority to Operate (ATO) letters, FISMA Reports, Standard Operating Procedures (SOP), in accordance with Federal, Agency and Organizational policy, to include FISMA, NIST, OMB, FIPS instruction. Possessed in-depth ability performing information security risk assessments and analysis, risk mitigation in large-scale networked application environments. Performed risk analysis, assessment testing and analysis utilizing tools

such as Nessus and others to support the testing process. Testing and Assessing Network Infrastructures, Data Warehouses, Web Applications (custom and commercial), Oracle Databases, Application Servers, Windows and Unix/Linux systems. Possess excellent analytical/strong initiative and qualifications required to excel and succeed. Continuously upgrading and readily prepared to take on new challenges, absorb and easily adapt to any emerging technology. SKILLS Security Assessment & Authorization, Certification & Accreditation, Security Planning, Vulnerability Scanning, Business Continuity Planning, Risk Assessments, Vulnerability Management, Penetrating testing, PCI (DSS), Security Test & Evaluation, Security Training & Awareness, Incident Response, Policy and Process Development, POA&M Management, MYSQL, MSSQL Server, Access, SharePoint, Oracle, VM ware, Mainframe- RACF, Windows, Unix / Linux, TAF, IDEA, CSAM, XACTA IA Manager, NESSUS, Microsoft SharePoint.

Name: Amber Bell

Email: lewisrichard@example.net

Phone: 001-334-297-8122x0229