Information Security Analyst Information Security Analyst Information Security Analyst - Premier LLC Frederick, MD Specialized in areas such as Security Assessment and Authorization (SA&A), Risk Management, System Monitoring, Regulatory Compliance, Physical and environmental security, Incident Response, and Disaster Recovery. Expert in FISMA, SOX 404 compliance, development of security policies, procedures and guidelines. I am a fast learner, easily adapt to new working environment and possess very good analytical and organizational skills. I have the ability to multi-task, work independently and as part of a team. Work Experience Information Security Analyst Premier LLC May 2016 to Present Maryland Analysed and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M) Assist System Owners and ISSO in preparing certification and Accreditation package for companies' IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 Designate systems and categorize its security objectives (Confidentiality, Integrity, and Availability) using FIPS 199 and NIST SP 800-60 Conduct Self-Annual Assessment NIST SP 800-53A Perform Vulnerability Assessment to make sure that risks are assessed, evaluated and proper actions have been taken to limit their impact on the Information and Information Systems 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 I.T 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 IT Compliance Analyst Forward Air Inc April 2015 to May 2016 New Jersey Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. 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). Developed system

security plans to provide an overview of federal information system security requirements and described the controls in place or to meet those requirements. Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk assessments (RAs), Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs). Prepared Security Assessment and Authorization (SA&A) packages to ascertain that management, operational, technical, and privacy security controls adhere to NIST SP 800-53 standards. Performed vulnerability assessment, making sure risks are assessed and proper, actions taken to mitigate them. Conduct IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports. These reports identified threats and vulnerabilities. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level. IT Auditor Swissport North America Inc June 2014 to March 2015 New Jersey Work closely with engagement manager to perform planning in accordance with business risks, staffing resources and time budgets to determine the scope of work. Obtain a comprehensive understanding of the location's IT environment, operations, and systems. Supervise all aspects of engagement execution, including planning and conducting opening and closing meetings with clients. Counsel, direct, and supervise the audit staff throughout the engagement. Review their work on a timely basis for adequacy and communicate possible improvements to staff. Ensure adequate workpapers and other supporting documentation is gathered and documented to analyse and evaluate the control environment. Identify control weaknesses, assess the impact of the weakness, and formulate effective and practical corrective actions for clients. Manage the creation and the consolidation of the audit report for review by Internal Audit Management in accordance with agreed upon timeframes. Address any questions or comments. Monitor the progress of corrective actions and follow-up with clients where appropriate. Participate in special projects in the department where appropriate. Actively pursue continuing professional education in line with the department's needs

and the auditor's career development. Prepare staff evaluations for review by engagement manager. Discuss evaluations with staff where required. Ensure all workpapers are reviewed and closed at the completion of the audit. IT Auditor Hilton Hotel - Woodbridge, NJ June 2013 to June 2014 Assist in audit engagement planning and reporting activities. Coordinate, plan and execute audit activities within the organization. Develop and implement complex audit test plans. Determine audit scope and objective and accordingly prepare audit work plan. Identify critical risks and recommend corrective steps to address the risks. Coordinate with business, finance, project and compliance teams to obtain inputs for audit processing. Develop auditing program to offer comprehensive audit coverage within the organization. Set audit priorities and determine the time required to complete each audit assignment. Adhere to auditing standards established by the company's audit department. Communicate audit findings and recommendations to Audit Manager. Ensure that previous audit recommendations are addressed and implemented. Develop well-crafted audit reports including results and recommendations for management. Schedule meetings with management to clearly understand the company processes and policies. Address auditing and operational issues in promptly. Identify best practices to meet audit requirements in a timely manner. Maintain clear and complete IT audit documentations. Education Associate Degree in Computer Science in Computer Science Union County College - Cranford, NJ 2013 Associate Degree in Information Technology in Information Technology Ghana Telecom University College - Accra, GH 2010

Name: Richard Taylor

Email: nsmith@example.org

Phone: 001-458-902-1643x094