IT Security Analyst IT Security Analyst IT Security Analyst - Comcast Corporation - MD Hagerstown, MD 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. Results-driven with notable success in the planning, analysis, and implementation of security initiatives with 5 years of experience in fast-paced environment. Strengths in providing security initiatives, comprehensive network design and security frameworks. Work Experience IT Security Analyst Comcast Corporation - MD February 2017 to Present   Developed a system security plan to provide an overview of information system security requirements and described the controls in place or planned   Developed risk assessment reports. These reports identified threats and vulnerabilities applicable to systems. 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   Developed an E-Authentication report to provide technical guidance in the implementation of electronic authentication   Led in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officers (ISSOs), the System Owners, the Information Owners and the Privacy Act Officer   Assisted in the development of an Information Security Continuous Monitoring Strategy to help in maintaining an ongoing awareness of information security (Ensured continued effectiveness of all security controls)   Assisted in the development of rules of engagement documentation in order to facilitate the scanning of network, applications and databases for vulnerabilities   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 a security baseline controls and test plan that was used to assess implemented security controls   Conducted kick off meetings in order to categorize systems according to NIST requirements of Low, Moderate or High system Information Security Analyst Smartthink Ltd (N.C.I) - MD May 2013 to February 2017   Analyzed and updated

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)   Assisted System Owners and ISSO in preparing certification and Accreditation package for company's 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   Designated systems and categorized its C.I.A using FIPS 199 and NIST SP 800-60   Conducted Self-Annual Assessment (NIST SP 800-53A)   Performed Vulnerability Assessment, making sure that risks are assessed, evaluated and a proper action 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   Performed IT risk assessment and documented the system security keys controls   Met with IT team to gather evidence, developed test plans, testing procedures and documented test results and exceptions   Designed and Conducted walkthroughs, formulated test plans, test results and developed remediation plans for each area of the testing   Wrote audit reports for distribution to management and senior management documenting the results of the audit   Participated in the SOX testing of the General Computer Controls   Evaluated client's key IT processes such as change management, systems development Senior Auditor First Data - MD June 2010 to July 2013   Facilitated financial and operational audits, working with internal and external managers to communicate recommendations or issues surrounding audits.   Identified management control weaknesses and provided value added suggestions for remediation.   Identified control gaps in processes, procedures and systems through in-depth research and assessment and suggested methods for improvement.   Established internal control systems by updating audit programs.   Developed and implemented corrective actions to bring business areas in line with standards.   Determined financial and operational audit areas, providing most economical and efficient use of audit resources.   Prepared working papers, reports and supporting documentation for audit findings.   Interviewed business owners, explained audit scope and conducted exit interviews of audit findings.   Evaluated design and operating

effectiveness of audit areas, including efficiency, effectiveness, and mitigating controls.   Facilitated financial and operational audits, working with internal and external managers to communicate recommendations or issues surrounding audits. Staff Accountant First Data - GA March 2006 to June 2010   Reconciled discrepancies between accounts receivable general ledger account and accounts receivable trial balance account.   Reconciled vendor statements and handled payment complaints or discrepancies.   Balanced monthly general ledger accounts to accurately record cost and month end accruals.   Researched and resolved accounts payable discrepancies.   Composed effective accounting reports summarizing accounts payable data.   Maintained up-to-date knowledge of tax codes, legislation and tax programs.   Performed advanced reviews of business operational trends and expected obligations to prepare accurate forecasts.   Generated and submitted invoices based upon established accounts receivable schedules and terms.   Maintained up-to-date knowledge on permits, certificates and documents mandatory for government departments. Education Master of Science Maryville University - St. Louis, MO February 2020 Bachelor of Science in Accounting Mount St. Mary's University Emmitsburg - Emmitsburg, MD 2014 Bachelor of Science in Finance University of Maryland University College - Adelphi, MD Associate of Science in Business Administration Frederick Community College - Frederick, MD Skills Security, Access control, Authentication, Oracle, Ms office, System security, Vulnerability assessment, Cash flow, Budget analysis, Financial modeling, Financial reporting, Gaap, Reconciliation, Risk management, Budget, Statutory reporting, Regulatory compliance Additional Information   Perform Certification and Accreditation documentation in compliance with company standards   Develop, review and evaluated System Security Plan based NIST Special Publications   Perform 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   In depth knowledge of COOP, COSO and COBIT Frameworks   Compile 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 Skills Expert in GAAP and statutory reporting Risk Management System Monitoring & Regulatory Compliance Vulnerability Assessment Authentication and Access Control Financial reporting specialist Financial modeling capability Network & System Security Oracle proficiency Superior attention to detail Cash flow analysis Blackline reconciliation MS Office Suite Budget analysis

Name: Stephen Hughes

Email: rogersalexis@example.org

Phone: 8852598789