Cyber Security Policy and Compliance Analyst Cyber Security Policy and Compliance Analyst Cyber Security Policy and Compliance Analyst New Carrollton, MD Within US Clearance: Public Trust Type of position: Full time Willing to Relocate: Yes Status: US Citizen Highest Degree attained: MS, MBA OBJECTIVE Seeking Senior IT Auditor position in your establishment with focus on FISMA, SOX 404, FISCAM, ISO, Privacy Act, HIPPA compliance, system security auditing, monitoring, risk analysis and assessments, audit engagements, testing of information technology security controls and mitigating risks, vulnerabilities, threats and exposure. STANDARDS/FRAMEWORK FISMA, COSO/COBIT, Sarbanes-Oxley Act (SOX), SAS-70/SSAE 16, ITIL, ISO 27001/27002, Payment Card Industry Data Security (PCI(DSS)), Privacy Act of 1974, HIPAA, Certification and Accreditation, Project Management, Change Management, OMB Circular A-130 Appendix III, NIST 800-53, NSA Guide, FIPS, STIG, DIACAP, FISCAM, Fed RAMP. Authorized to work in the US for any employer Work Experience Cyber Security Policy and Compliance Analyst Booz Allen Hamilton (Department of Veteran Affairs (VA) November 2014 to Present Functioned as a Security Analyst on VA Materials Weakness Remediation Support (MWRS) project where she reviewed and/or developed the security control implementation documentation details as required by NIST SP 800 publication series. Functioned as a Security Analyst on VA Assessment and Authorization (A&A) Artifact update and Wireless Scanning project. Functioned as the RiskVision (GRC tool) System Steward in the VA Mobile Infrastructure Service ATO (MIS) project. Participated in the VA Standardization of Implementation Facility Statements meetings. Developed Deficiency and Action Plan template for monitoring the deficiencies in the VA System Security Plans and Risk Assessment documentation in RiskVision and proffering remediation. Served as a key member of dynamic team providing A&A support to VA with the review, enhancement and development of VA's System Security Plans (SSPs) and Risk Assessments (RAs), in accordance with federal requirements and agency A&A policy. Provided A&A support to the system's VA Information Security Officers (ISOs) and System Owners in a fast-paced environment where processes are ever changing to meet VA and Federal technical security requirements. Travelled to and conducted on-site facility system security plan compliance reviews and provided remediation implementation statements to answer

security control questions in different VA regions. Assisted with informing VA staff and leadership of A&A policy, guidance, and security responsibilities based on specific VA security roles / titles. IT Security Auditor Smart Think Inc October 2012 to October 2014 Conducted a kick off meeting in order to categorize organization's systems according to NIST requirements of Low, Moderate or High system Developed a security baseline controls and test plan that was used to assess implemented security controls Developed key security standards by performing an in-depth assessment of CMS information systems in order to maintain FISMA and HIPAA compliance by implementing guidelines and standards identified in the National Institute of Standard and Technology (NIST) 800 series in facilities throughout each US state and District of Columbia. Created a repository for the deliverables. Completed assessment and generated security assessment report detailing the results of the assessment by location along with the plan of action and milestones (POA&M). Developed Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA) where personal identifiable information is identified. IT Security Auditor February 2011 - September 2012 Smart Think Inc. (National Institute of Health (NIH) Was a team member of the Center for Information Technology tasked with conducting Certification and Accreditation (C&A) on applications within NIH using the six steps of the Risk Management Framework (RMF) from NIST SP 800-37 in order to meet the necessary Federal Information Security Management Act (FISMA). All information (artifacts/evidence) collected was attached or entered into the NIH Certification and Accreditation Tool (NCAT) which utilizes NIST SP 800-53A rev. 1 and NIST SP 800-53 rev.3. Credentialed Nessus and AppScan results were analyzed to determine the security posture of each application as applicable. At the end of the assessment NCAT generated a package which included the System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms that was presented to the Designated Approving Authority (DAA) in order to obtain the authority to operate (ATO) Evaluated the adequacy of internal controls and compliance with company policies and procedures by conducting interviews with all levels of personnel, examining transactions, documents, and performing walkthroughs. Provided support and guidance through all phases of C&A process, including monitoring C & A artifacts compliance (FIPS 199/200, PIA, SORN, Risk

Assessment, Security Test and Evaluation (ST&E), Security Assessment Report (SAR), vulnerability scans, annual contingency plan testing, and POA&M management Developed baseline configuration standards for servers used by the center for information Technology within NIH. IT Security and Compliance Analyst MJHS Corporation Group July 2009 to January 2011 Conducted IT 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 (PCI-DSS). Acted as Security Project Manager by facilitating efficient communication across all levels of information assurance project team to ensure consistency in reaching the project's goals and to help in the recognition of any potential opportunities, risks or complications. Assisted in the development of information Security Continuous Monitoring Strategy in maintaining an ongoing awareness of information security, vulnerabilities and threats to support organization's risk management. Performed Contingency Planning and Contingency Planning Test annually Performed evaluation and tests in the areas of security, operations, and change management. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning, and Relationship with Outsourced Vendors Identified gaps, developed remediation plans, and presented final results to the IT Management team Education Masters in Science University of Maryland University College Masters in Business Administration in Management University of Calabar Bachelor of Science in Library Information Science University of Nigeria Nsukka Skills Certification and Accreditation (5 years), Risk Assessment (5 years), Security (6 years), Compliance, Policy Analysis (5 years), Gap Analysis (6 years) Certifications/Licenses CompTIA A+ January 2015 to January 2018 Additional Information I am an ingenious, resourceful and detail oriented individual with specialization in areas such as Network security, Cyber security, Information Assurance (IA), Certification and Accreditation (C&A), Risk Management, Authentication & Access Control, System Monitoring, Regulatory Compliance, Physical and environmental security, Project Management, Incident Response, Business continuity and Disaster Recovery. I possess a strong managerial skill, excellent in building relationship and developing strategic partnership. I am very

good in identifying gaps between current/desired capabilities and existing documentation; developing and executing a plan to develop the required documentation to enhance agency security capabilities. I am an expert in FISMA, SOX 404, SANS20, ISO 27001/27002, PCI-DSS, or HIPPA IT controls compliance, security training, developing system security plan, policies and procedures. I am highly adaptive and have superior analytical and organizational skills as well as familiar with a wide variety of applications, databases, operating systems and network devices. I am a fast learner, have the ability to multi-task, and can also work independently and as a contributing team member. I have a strong verbal/written communication skills and technical writing skills. I have more than Six (6) years of experience in information security and Information technology audit.

Name: Elizabeth Edwards

Email: brownpeter@example.org

Phone: (478)300-3942x231