

Compliance Analyst, Cybersecurity Compliance Analyst, Cybersecurity Compliance Analyst, Cybersecurity Maple Grove, MN Work Experience Compliance Analyst, Cybersecurity Javen Technologies - Abbott Laboratories Inc - Saint Paul, MN February 2018 to June 2019 Performed detailed security risk assessments of Abbott (CAT-legacy) as directed; facilitated product security remediation efforts to successful completion. Performed detailed cybersecurity maintenance plans and reports (CSMP & CSMR) of Abbott (CAT-legacy) as part of the product security remediation efforts to successful completion. Performed detailed Manufacturer Disclosure Statement for Medical Devices Security (MDS2) of Abbott (CAT-legacy) as directed to facilitate and enhance easy use by customers. Supported cybersecurity remediation activities for (CAT-legacy) fielded products. Participated in product security efforts including: asset identification, asset remediation disposition, risk assessment activities and product remediation support. Research formal documentation as it pertains to asset management process identified by the Senior Security Compliance Analyst for Abbott (CAT-legacy) fielded products. Participated in the cybersecurity remediation project planning and implementation efforts; perform audit related activities such as DHF cybersecurity documentation and evidence gathering; create, maintain, and continually improve documentation for product security compliance per the Cybersecurity Risk Management WI;

Provided security knowledge and assisted in identifying potential vulnerabilities and control measures applicable to fielded product. Developed product security compliance technical documentation for internal and external use; Developed technical expertise pertaining to product security and effectively transfer knowledge to business and IT team members; IT Compliance Analyst Cokem International - Shakopee, MN June 2015 to December 2017 Developed security control test plans and conducted in-depth security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and policies safeguards in order to maintain HIPAA compliance. Developed HIPAA compliance reports documenting auditing finding and corrective actions. These reports were submitted to the ISSO. Involved in the security awareness and training of staff on HIPAA requirements as it related to information technology. Conducted Certification and Accreditation (C&A) on general support system and major application

using the six steps of the Risk Management Framework (RMF) from NIST SP 800-37. Developed System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms that were presented to the Designated Approving Authority (DAA) in order to obtain the authority to operate (ATO) Conduct a Business Impact Analysis (BIA) to identify high risk area where audit effort will be allocated. Conducted meetings with the IT client team to gather evidence, developed test plans, testing procedures and documented test results and exceptions. Conducted walkthroughs, formulated test plans, documented gaps, test results, and exceptions; and developed remediation plans for each area of testing. Performed IT operating effectiveness tests in the areas of security, operations, change management, and email authentication. Developed the audit plan and performed the General Computer Controls Testing Identified gaps, developed remediation plans, and presented final results to the IT Management team. Initiated and lead information security awareness and training programs. Information Security Analyst Cokem International - Bronx, NY June 2015 to December 2016 Conducted IT controls risk assessments that included reviewing organizational policies, standards, procedures and guidelines. Developed a security baseline controls and test plan that was used to assess implemented security controls. Developed and conducted ST&E (Security Test and Evaluation) according to NIST SP 800-53A Conducted a security control assessment to assess the adequacy of management, operational privacy, and technical security controls implemented. A Security Assessment Report (SAR) was developed detailing the results of the assessment along with plan of action and milestones (POA&M) to the Designated Approving Authority (DAA) to obtain the Authority to Operate (ATO). Assisted in the development of an Information Security Continuous Monitoring Strategy to help DFA Inc. in maintaining an ongoing awareness of information security (Ensure continued effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions.

Assisted in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officer (ISSO), the System Owner, the Information Owners and the Privacy Act Officer Education MBA St. Mary's University of Minnesota School of Business and Technology - Minneapolis, MN October 2016 Bachelor of Arts

degree in Psychology/ Information Technology University of Ghana - Accra, GH September 2009

Name: Nicole King

Email: joshua18@example.org

Phone: 001-885-688-5276x61554