IT Compliance Analyst IT Compliance Analyst IT Compliance Analyst - MARTIN POLLAK PROJECT INC Baltimore, MD Work Experience IT Compliance Analyst MARTIN POLLAK PROJECT INC August 2017 to Present Conducted kick off and bi-weekly meetings with the system owners, ISSO, Admins, and the assessment team members prior to Assessment engagements to gather evidence and deliverables about the control environment and vulnerabilities discovered. Meet with system owners and stakeholders to identify assessment scope and attain artifacts needed for successful completion of assessments. Collaborating with stakeholders for pre and post Assessment and Authorization (A&A) activities. Coordinate and execute projects and ensured security risks/vulnerabilities are identified, communicated and remediated. Assessed a subset of the Access Control, that's AC-2, AC-3, AC-5, and AC-6 by reviewing account system generated reports in accordance with the organization-defined monitoring strategy and ensures that the organization follows the policies and procedures Plan, manage and execute the IT audit functions using best practice audit guidelines in compliance with COSO and COBIT. Work closely with management (IT Directors, Managers, etc.), over IT audit findings, compliance issues, recommendations, management's response and implementation. Establish IT compliance frame work covering IT platform applications, processes and procedures to ensure compliance with industry standards and best practices. Supported the Risk Team to perform gap analysis and provided risk mitigating strategies, helped prepared and submitted the necessary documentation to management. Measure the adequacy of the quality of IT service delivery, through the review of key controls in incident management (help desk), problem, and release and change management. Serve as the RMF Assessor Maintain Day-to-Day security analysis of the package to ensure timely updates and notifications Ensure projects plans are updated for significant changes to scope, cost, and schedule and resource usage; and are agreed to by all parties. Recommend process improvements on vulnerabilities tracking and possible remedy to security issues. Perform follow-up on every past due resolution. Communicate with client-facing Information Assurance support as an Information System Compliance Analyst on behave of Martin Pollak Project. Conduct and perform continuous monitoring in relation to the NIST SP 800-137, 800-37, 800-53

&53A, 800-171&171A, ISO 27001&2 and client's requirements. Assess for compliance within client's using the NIST SP 800-53 A rev. 4, SP 800-171A, and ISO 27001/2. Perform security assessments on controls inherited and within the systems. Using the methods of conducting assessment such as testing, interviewing and examining, I validated the controls with the evidence using the "determining if" statement and the control description. Develop, review and perform update on the security authorization package documents like the SSP, SAR and POA&M in accordance with NIST requirements. Moderated weekly POA&M Corrective Action Meetings to implement recommended risk mitigation strategies. US SECURITY ASSOCIATE February 2013 to August 2017 Security Information Analyst /Assessor Conducts kick-off and bi-weekly meetings with system owners, ISSO, administrators, assessors, and other IT team members prior to assessment engagements to gather documentation, artifacts, and evidence about their control environment and vulnerabilities discovered. Work with stakeholders to ensure the identified weaknesses from vulnerability scans are remediated in accordance with defined remediation time frames to satisfy SI-2 Control. Developed Security Assessment Reports and providing sound remediation guidance, and prepare training conferences, exercises, and video teleconferences to meet annual IA training objectives. Developed, reviewed and updated Information System Security Plans (SSP), Contingency Plans (CP), Configuration/Change Management Plans (CMP), and Privacy Impact Analysis (PIA) using the appropriate NIST Publication and industry best security practices. Developed Security Authorization documents including, System Security Plan (SSP), Security Assessment Plan (SAP) and Plan of Action and Milestones (POA&M) in accordance with NIST guidelines. Reviewed System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M). Analyzed the Security Assessment Reports (SAR) and provided feedback to stakeholders as to closing POAM. Conduct security assessments in accordance with current NIST and DHS guidance, as well as client policies and procedures for all client systems and applications. This may include Major Applications (MA), General Support Systems (GSS), subsystems, minor applications, and other information systems. Develop SAPs, test the documented systems in accordance with applicable policies and guidelines, and document results of

the testing in the Risk Traceability Matrix Assess up to 8 individual systems simultaneously per federal government schedule Established and enforced security policies to protect the organization's computer infrastructure, networks and data Evaluated the effectiveness of existing security measures, such as firewalls, password policies and intrusion-detection systems Gathered and organized technical information about an organization's mission goals and needs, existing security products, and ongoing programs in computer security Information Risk Analyst RITE AID INC August 2012 to February 2013 Work closely with developers to identify the appropriate certification/approval processes and authorities. Reviewed, analyzed and evaluated the security controls used to protect the data of the organization. Review and analyze the findings that identify security issues on the system and compile results and finding into a final Security Assessment Report, along with assessments and recommendations for remediation. Reviewed, maintained and updated remediation on (POAMs) within the organization by working with POAM owners to resolve POAMs, gathering artifacts and close the POA&M. Supported the organization in the development, oversight, and maintenance of security compliant programs. Supported the Security Assessment and Authorization (SA&A) compliance, NIST requirements and continuous monitoring for Security Controls. Operate Risk Management Framework using Confidential 800 - 37 as Confidential guide and FIPS 199 as Confidential guide to categorize information systems. Classify information Systems using the RMF processes to ensure system Confidentiality, Integrity and Availability. Select security controls using Confidential 800-53 Rev 4 as guidance base on system security categorization. Ensure that controls are implemented correctly, functioning as intended and producing the right results Document selected security controls in the SSP that was earlier created using Confidential 800-18. Determine likelihood of risk occurrence using Confidential 800-30 as Confidential guide Most of my current projects are focused on RMF phase 4 (Assessing security controls) Effectively engage in the assessment processing & preparing for assessment, conducting assessment, communicate assessment results, and maintain the assessment. Coordinate, participate and attend weekly Confidential forums for security advice and updates. Use the implementation section of the (SSP) System Security Plan in addressing how each control

is implemented (frequency of performing the controls, control types and status). Create SAP (to document assessment schedules, control families to be assessed, control tools and personnel, client's approval for assessment, assessment approach and scope, ROE if vulnerability scanning is involved). Determine assessment method (examining policies and procedures, interviewing personnel and testing technical controls), using Confidential 800-53A as Confidential guide. Create (RTM) and Risk Traceable Matrix in which to document assessment result (pass/fail) Prepare Security Assessment Reports (SAR) in which all the weaknesses are reported. Skills Cobit, Hipaa, Iso, Iso 27001, Nist, Pci, Sox, Security, Access control, Fisma, Assurance analyst, Information assurance, Sas, Sdlc, Sarbanes-oxley, Sarbanes-oxley act, Security plan, System security, Sar, Audit Additional Information SKILL SUMMARY Highly efficient and task Oriented Information Assurance Analyst skilled in Microsoft Excel, Microsoft Word, NIST SP 800 series, RMF, Cloud Services, compliance verification, and developing Authorization package including but not limited to System Security Plan (SSP), Plan of Action and Milestone (POAM) and Security Assessment Report (SAR). As a security control analyst, my goal is to always deliver high quality results and prospects. Career oriented professional with solid experience in Information Assurance analysis, compliance documentation and administration. CORE STRENGTHS NIST SP 800-53A, FISMA, Cloud Services (FedRAMP), COSO/COBIT, Sarbanes-Oxley Act (SOX 404), SAS-70, SSAE 16&18, PCI-DSS, Access Control, Audit and Accountability, HIPAA, ISO 27001/2, HITRUST, SDLC, Assessment and Authorization (A&A), Certification and Accreditation (C&A), FISMA, FedRAMP, OMB A-130, A-123, FIPS 199 & 200.

Name: Ann Ward

Email: nichole94@example.com

Phone: 001-210-307-6369x27727