Job Seeker Buffalo, NY A Proficient Cyber Security Analyst with 5+ years of experience focusing on the implementation of the Risk Management Framework(RMF) starting from System categorization, security control selection, implementation, assessment, authorization and Monitoring of security controls in an effort to mitigate information system risk. Work Experience Brown Brothers Harriman & Co., Jersey City May 2019 to August 2019 Information Risk Security Management ? Designing and implementing an overall risk management process for the organization, which includes an analysis of the financial impact on the company ? Performing a risk assessment and evaluation ? Administer user systems and data entitlements, across multiple platforms and applications ? Preparing risk management and insurance budgets ? Coordinate with local security coordinators and application data owners to ensure access to programs and applications are processed and verified, within the most current standards and requirements ? Perform first level ISM user system access requests with a 95% in 24 Hours Service Level Agreement. ? Used programming languages such as Java, JavaScript, PowerShell, Perl, PL/SQL, Active Directory to write scripts to automate repetitive tasks and assist with global automation ? Conducting policy and compliance audits, which will include liaising with internal and external auditors ? Creating business continuity plans to limit risks ? Building risk awareness amongst staff by providing support and training within the company IT Security Analyst AlphaHill, LLC February 2017 to May 2019 Conduct comprehensive assessments of the management, operational and technical security controls employed within or inherited by the system to determine the overall effectiveness of the control and ensure that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system ? Conduct security assessments on assigned systems and collaborate with clients to provide recommendations regarding critical infrastructure, network security operations, and Continuous Monitoring processes ? Collaborate with ISSOs to ensure systems are properly categorized, their controls selected and implemented based on the systems categorization level ? Create, update, and revise System Security Plans, FISMA, Contingency Plans, Incident Reports and Plan of Action & Milestone ? Participate in A&A Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) per NIST SP 800-53A ?

Document and finalize security Assessment Report (SAR) in preparation for ATO ? Collaborate with SOC engineers to perform continuous monitoring of systems to ensure security and compliance. ? Determine security controls effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements). ? Evaluate threats and vulnerabilities based on Nessus tenable reports and also Implement Risk Management Framework (RMF) in accordance with NIST SP 800-37. ? Classification and categorization of information Systems using the RMF processes to ensure system Confidentiality, Integrity and Availability. ? Provide audit briefings to agency and Information Systems Security Officer's (ISSO), to assist in the preparation of independent audit assessments with the agency's goal of improving their operational effectiveness and ensuring that all findings are documented as Plan of Action & Milestones. ? Used MS Systems Center Operations Manager to monitor the health of all Windows servers and all the applications that run on them. ? Used SNMP to receive alerts from hardware and applications ? Developed and Supervised security awareness training activities for junior security analysts Acethia MD January 2015 to January 2017 ISSO ? Created and fine-tuned information security policies that supported the objectives and requirements defined in the company security plan ? Reviews security controls in accordance with the NIST SP 800-53 controls and generates compliance status reports; ? Collaborate with System Owners to categorize systems, select controls, implement controls, and ensure that systems are assessed, authorized, and monitored. ? Evaluates new IT systems involving software, hardware, configuration, and proposed changes to ensure IT security posture is in compliance with existing information security policies and regulations; ? Coordinates resolution of system deficiencies and POA&M findings with stake holders as required; ? Prepares plan of action and milestones (POA&M) reports to record system deficiencies and findings for all DS applications ? Reviews and validates system configurations to ensure that a suite of security and compliance software, hardware and related toolsets are in accordance with appropriate risk management framework design; ? Performs continuous monitoring activities on new and existing systems and networks ? Update security policies and procedures on assigned systems to ensure compliance on FISMA regulations Junior Security Assessment Analyst Infos Pro Solutions, LLC January 2014 to

December 2015 Collaborate with the assessment team to perform security controls assessments using NIST SP 800-53A as a guide to Interview, Examine, and Test systems. ? Work as part of the assessment team to determines Technical, Operational and Management security controls effectiveness by assessing if controls are implemented correctly, operating as intended, and meeting security requirements. ? Schedule assessment kick-off meetings with the ISSO, System Owners, and stakeholders. ? Creates Requirement Traceability Matrix (RTM) and documents whether assessed controls passed or fail using NIST SP 800-53A as a guide. ? Creates and finalizes Security Assessment Report (SAR) and give recommendations to ISSO on how to mitigate or remediate reported weaknesses and vulnerabilities. ? Reviews A&A package items using NIST guidance for FISMA compliance such as the System FIPS 199 Categorization, e-Authentication Assessment, PTA, PIA, Contingency Plan (CP) and Contingency Plan Test (CPT) Education Bachelor of Science in Engineering University at Buffalo, The State University of New York May 2018 Skills Active directory, Fisma, Pci, Iso, Iso 27001, Nist, Siem, Splunk, Adfs, C#, C++, Javascript, Perl, Python, Sharepoint, Pl/sql, Sql, Java, Cyber security, Identity management Additional Information Summary of Skills Conversant in FISMA, NIST and FIPS publications. Especially NIST 800-37, NIST 800-53 Rev 4, NIST 800-53a Rev 4 Knowledgeable in the ISO 27001 Framework used in securing systems in international organizations Conversant in the PCI DSS Framework used in security systems in the Financial industry Knowledgeable in vulnerability management and compliance regulations Experienced in the NIST RMF process used for managing cyber security risk Experienced working with SAML, and SIEM tools like Splunk, and ArcSight as an analyst Experienced with managing windows file shares permissions Experience with Sailpoint identity Management Experienced in programming tools using C#, C++, Perl, Python, Unix Shell Scripts, PowerShell, Java, JavaScript, PowerShell, and PL/SQL Experienced with ADFS, MS Azure, Sharepoint access management and Active Directory Experienced with implementing and administering group policy object Ability to adapt in a fast paced and time sensitive environment Excellent analytical and problem-solving skills in designing, developing, and implementing security standards Highly organized, Self-motivated and responsible for assigned

tasks

Name: James Klein

Email: wernerjoseph@example.net

Phone: 571-832-5968