IT SECURITY ANALYST IT SECURITY ANALYST IT SECURITY ANALYST - EZEK SYSTEMS LLC Landover, MD Over six (6) years of experience in IT Security positions within Commercial and Federal organizations, leading and managing network security, vulnerability management, intrusion detection, Risk Management, Security Planning, Security Assessment & Authorization, Certification & Accreditation with in-depth knowledge of applying, NIST 800-53, FISMA, SDLC, ISO 27001, SANS -20 guidelines to comply with various private and federal agencies. FUNCTIONAL AND TECHNICAL SKILLS: NIST 800-53, ISO 27001, Sans-20, Assessment of Internal Controls, IT Incident Analysis, FISCAM & FISMA Audits, IT Security and Risk Management, Security Assessment & Authorization, Certification & Accreditation, Security Planning, Vulnerability Management, Security Test & Evaluation and Policy & Process Development, Microsoft Word, Excel, SharePoint, Oracle Financial, TAF, IDEA, CSAM, ACL and NESSUS Work Experience IT SECURITY ANALYST EZEK SYSTEMS LLC May 2016 to Present In depth Knowledge of National Institute of Standards and Technology Special Publication (NIST SP) documentation: Performed assessments, POAM Remediation, and document creation using NIST SP 800-53 Rev.2 and NIST SP 800-53 Rev.4. Knowledge of Several Computer Environments: Performed evaluation and guidance on security control implementation on multiple environments include Windows server, Windows 8, Windows XP, Solaris, Oracle, Cisco IOS, custom created applications, and COTS applications and windows 2012 R2 Security Documentation: Performed updates to System Security Plans (SSP), Risk Assessments, and Incident Response Plans, create Change Control procedures, and draft Plans of Action and Milestones (POAMs). Training of clients and coworkers: Created training decks to train clients and coworkers on processes at the client site. Additionally, ran training sessions, using the created deck, on how to process POAMs, function requirements, and NIST control mappings. POAM Remediation: Performed evaluation of policies, procedures, security scan results, and system settings in order to address controls that were deemed insufficient during Certification and Accreditation (C&A), RMF, continuous monitoring, and FISCAM audits Develop Solutions to Security weaknesses while working on POAM remediation and Corrective Action Plan (CAP). Assists the ISSOs to create solutions to weaknesses based on system

functionality and pre-existing architecture. Communicates between multiple clients by acting as the single point of contact for clients in regards to POAM remediation and CAP remediation. Handling of internal communications within Office of Information Security and external communications with several different divisions on a daily basis. Maintain excellent working relationships with both internal and external customers using communication skills. Risk Management Framework (RMF) assessments and Continuous Monitoring: Performed RMF assessment on several different environments using both scanning tools and manual assessment. Assessment included initiating meetings with various System Owners and Information System Security Officers (ISSO), providing guidance of evidence needed for security controls, and documenting findings of assessment. Conducts Security Risk Assessment on all new applications, IT Systems or changes to existing IT systems to verify that they satisfy established security baseline before adoption into VA (Virginia) Regional offices. Conduct Security Risk Assessment on new Vendors and annual Vendors' Risk Assessment. Assist management in authorizing the IT Systems for operation on the basis of whether the residual risk is at an acceptable level or whether additional compensating controls should be implemented. Ensure compliance with Baseline security configurations, IT controls and policy standards. IT/ INFORMATION SECURITY ANALYST SYNERGY TAX AND FINANCIAL SERVICES November 2014 to April 2016 Conducting meetings with the IT team to gather documentations and evidences (Kick-off meeting) about their control environment. Performing Security Categorization using FIPS 199 and NIST 800-60 Vol 2, Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders. Developing and maintaining Plan of Action and Milestones (POA&MS) of all accepted risks upon completion of system Assessment and Authorization (A&A) Creating, updating and revising System Security Plans, Contingency Plans, Incident Reports and Plan of Action & Milestone Conducting risk assessments regularly; ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37 Conducted FISMA-based security risk assessments for government contracting organizations and application systems, including interviews, tests and inspections; produced assessment reports and

recommendations; conducted out-briefings. Assessments conducted following NIST 800 processes and controls. Supporting clients in creating a memo for findings that has passed Scheduled Completion Date. Supporting clients in creating Risk Base Decision (RBD) for Plan of Action and Milestones (POA&M) that passed Scheduled Completion Date (SCD) Experience with NIST standard on cyber security and incident handling (800-63, 800-61) Provide continuous monitoring support for control systems in accordance to FISMA guidelines. Reviewing and updating Security Artifacts such as System Security Plan (SSP), Security Assessment report (SAR), Security Assessment Plan (SAP), contingency plan (CP), Privacy Impact Assessment (PIA), and Plan of Actions and Milestones (POA&M) Performing onsite security testing using vulnerability scanning tools such as Nessus Implementing and reviewing of ISO 27001: 2013 Controls in addressing security concerns in PCI DSS compliance Supporting client in creating Standard of Operation and Procedures (SOP) for systems as part of Plan of Action and Milestone. IT/ INFORMATION SECURITY ANALYST DOCUMENT SYSTEM INCORPORATED June 2011 to October 2014 Provide continuous monitoring support for control systems in accordance to FISMA guidelines. Maintained accountability of the entire computer resources in the company at all times. Performing onsite security testing using vulnerability scanning tools such as Nessus Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M), Authorization letter/memorandum (ATO). Reviewed and ensured Privacy Impact Assessment (PIA) document after a positive PTA is created. Updated Plan of Action & Milestones (POA&M) and Risk Assessment based on findings assessed through monthly updates. Education Bachelor of Science in Accounting University of Technology

Name: Robert Mason

Email: chad12@example.net

Phone: 883.684.0552x10094