

IT Security Analyst IT Security Analyst IT Security Analyst Lorton, VA Experienced in information assurance and security analysis. Proficient in Security Authorization process based on NIST RMF 800-37 Rev. 1. Coordinate in-depth interviews and examine documentation and artifacts in accordance with NIST 800-53A and 800-53 rev 4. Strong Leadership ability with proven aptitude to thrive in a team environment. Proficient in Microsoft Office. Excellent communication skills to include strong verbal and written skills, and very detail orientated. Ability to identify potential online security risks. This includes knowledge to compile daily database reports to ensure the security of the system. Also knowledgeable in common business-related IT functions. Authorized to work in the US for any employer

Work Experience

IT Security Analyst XO Communications September 2015 to Present

- Review IT security policies, procedures, standards and guidelines according to department and federal requirements using steps of the SA&A (Security, Assessment and Authorization)
- Review System Security Plan (SSP) and convert the SSP to latest templates for the assessment
- Develop assessment plans, assessment reports and post-assessment out-brief
- Conduct continuous monitoring schedule and assessment
- Develop Security Assessment Report (SAR) based on assessment results
- Conduct Security Testing based on NIST SP 800-53 Rev. 4, NIST SP 800-53A
- Coordinate A&A schedule with the assigned Information Systems Security Officer (ISSO) on deployment of new systems and modifications of legacy systems
- Conduct interviews with key client stakeholders to evaluate the current information security practices
- Conduct security control assessments within the ongoing authorization cycle
- Ensure that system security requirements are addressed during all phases

IT Security Analyst Crest Consulting Group November 2013 to September 2015

- Provided independent RMF Step 4 documentation review and security assessment services in support of A&A
- Executed Step 4 (Security Assessment) of the NIST Risk Management Framework (RMF)
- Documented the assessment findings in the Security Assessment Report (SAR)
- Developed recommendations for security issues during assessments
- Created detailed recommendations for compliance
- Scheduled and facilitated ad-hoc discovery sessions with the applicable stakeholders
- Reviewed and analyzed evidence to ensure each assessment objective is achieved
- Worked with stakeholders and system application team to

conduct interviews and collect artifacts relevant to assessment of security controls Maintained a good working relationship to enhance customer satisfaction Analyzed information security policies, procedures, standards, and guidelines using National Institute of Standard and Technology guidelines Documented findings in the SAR Security Control Assessor Paragon Systems February 2011 to November 2013 Conducted step 4 of (RMF) Risk Management Framework (Assessing security controls) Used the implementation section of the System Security Plan (SSP) to address how each control is implemented (frequency of performing the controls, control types and status) Created 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) Determined assessment method (examining policies and procedures, interviewing personnel and testing technical controls) using NIST 800-53A as a guide Created Requirements Traceable Matrix (RTM) to document assessment result (pass/fail) Prepared Security Assessment Reports (SAR) in which all the weaknesses are reported Determined threat sources and applied security controls to reduce risk impact Conducted risk management by identifying, assessing, responding to, and monitoring risk respectively Used POA&M tracking tools like CSAM (Cyber Security Assessment and Management), Excel spread sheet to make sure the POA&M is not in delay status Ensured that controls are implemented correctly, functioning as intended and producing the right results Education BS in Cyber Security Stratford University Skills testing, access, security Certifications/Licenses CAP Security+

Name: Frank Thomas

Email: bgarcia@example.org

Phone: 001-677-360-7694x7269