IT Security Analyst IT Security Analyst IT Security Analyst - HCL AMERICAN OCCIDENTAL PETROLEUM Houston, TX Detail-oriented IT Security Engineer with strong educational background in Engineering, supported by field research and professional work experience in Information Security Analysis, Governance Regulatory Compliance, SharePoint, & heterogeneous database environments. Authorized to work in the US for any employer Work Experience IT Security Analyst HCL AMERICAN OCCIDENTAL PETROLEUM June 2014 to Present 77046. Performed systems and network vulnerability scans to identify and remediate potential risk. Retina, Nessus and MBSA vulnerability scanners were used to detect potential risks on a single and on multiple assets across the enterprise network Used NIST SP 800-53A as guidelines to conduct Security Assessment. Utilized NIST SP 800-18 and updated System Security Plans from NIST SP 800-53. Developed and updated Plan of Action and Milestone (POA&M) for identified vulnerabilities and ensure compliance through monthly updates. Developed and conducted Contingency Plan and Testing Maintained inventory of all Information Security System assigned Ensured compliance to FISMA and NIST recommendations, as well as companywide security policies and procedures, and organizational guidelines and technical best practices. Developed a variety of Assessment & Authorization deliverables including; System Security Plan (SSP), Security Assessment Report (SAR), Contingency Plan (CP) and POA&M for review and approval by Authorization Official. Reviewed Privacy Impact Assessment (PIA), System Record of Notice (SORN), and initiated corrective measures when security vulnerabilities occurred. Implement Risk Management Framework (RMF) in accordance with NIST SP 800-37. Perform System security categorization using FIPS 199 & NIST 800-60 Advise Information System Owner (ISO) of security impact levels for Confidentiality, Integrity and Availability (CIA) using NIST SP 800-60 V2. 15511 TUCKERTON ROAD APT 105 HOUTON TEXAS 77095 Email: ltmorgen@yahoo.com Tell: 240 342 1212. Utilize NIST SP 800-18 and update System Security Plans from SP 800-53. Coordinated and managed team activities during Assessment engagement. Established schedules and deadlines for Assessment activities. Held kick-off meetings with CISO and system stakeholders prior to assessment engagements. Create reports detailing the identified vulnerabilities and the steps necessary to remediate them. Apply appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53 rev4, FIPS 199, FIPS 200 and OMB 130 Appendix III Information Assurance Analyst MODIS/HPE January 2014 to June 2016 Complied with the HIPAA Security Rule and PCI standards. Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Conducted Security Control Assessments to assess the adequacy of Management, Operational privacy, and Technical security controls implemented. Developed and maintained artifacts for A&A process that included but not limited to POA&M, SAP, SAR, RTM, CP, RA, PTA, CPT, & SSP. Planned System Security Checklists, Privacy Impact Assessments (PIA), POA&M, and Authority to Operate (ATO) letters. Assisted in the development and maintenance of System Security Plans (SSP) and Contingency Plans for all systems. Conducted IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards. Developed risk assessment reports, identifying threats and vulnerabilities. In addition, also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identify the overall risk level. Education Diploma in computer science VMT educational center focus Skills NIST (4 years), SECURITY (4 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (3 years), FISMA (3 years), DATABASE (Less than 1 year) Additional Information SKILLS IT Administration: Microsoft Windows Server 2008 & 2012, Linux Servers. Database: Microsoft SQL Server 2008 & 2012, Oracle, DB2. Using IDS/IPS and other SIEM tools to determine the existence and nature of security incidents, and create security incident tickets. Perform Vulnerability scanning and Penetration Test. Use NIST & FISMA guidelines to ensure overall organizational security compliance. ..

Name: Daniel Grant

Email: wallerjohn@example.net

Phone: 001-442-596-6297