IT Security Analyst IT Security Analyst Sr. IT Security Analyst - US EPA Office (OCFO) Alexandria, VA Authorized to work in the US for any employer Work Experience IT Security Analyst State of Alabama - Montgomery, AL December 2015 to September 2016   The CARES Project is an eligibility and enrollment services for life-critical support programs to families in need through State sponsored Medicaid, CHIP and DHR for Alabama State.   This was a $100m project spanning through multiple state agencies.   Worked with ISSM to ensure that management, operational and technical controls for securing sensitive security systems complied with special publication 800-53 requirements.   Assisted the System Owners and ISSM in preparing Certification and Accreditation packages for their IT systems   Reviewed and updated some of the artifacts especially FIPS 199 (SP 800-60), Initial Risk Assessment (SP 800-37), E-Authentication, PII, PTA, PIA, ST&E, SAR, and the POAM.   Ensured that Contingency Planning and Contingency Planning Test are carried. Conduct Annual Self-Assessments; identified and communicate IT audit findings to senior management   Established and documented compliance with information security policies and standards   Performed risk assessments for information technology assets using the risk management process and the process defined in the Federal Information Security Management Act (FISMA)   As a QA Engineer, I concentrate testing efforts on POAM highly critical eligibility system for Medicaid, Medicare, DHR and other federal and local government systems.   Participated in working Sessions and Reviews with ISSM, CCP IR Analysts, Security Assessors and other support staff on the project.   Performed Hub calls and document Requests and Responses from CMS through the coded UI and the CARES internal Test Harness.   Collaborated with Technology and Operations teams to communicate any application deficiencies/ bugs that are uncovered during testing, along with defect resolution. Security Analyst Bank of America - Atlanta, GA December 2008 to March 2010   Managed internal IT audit engagements including: system platform audits, PCI Compliance for the bank   Readiness reviews, IT Risk Assessments, change management, and business process control assurance   Managed security control assessments of Payment Systems for merchant boarding and settlement of funds.   Collaborated with Information Technology and Operations areas to proactively assess security policy compliance and monitor risk   Coordinated

external 3rd party auditors, including PCI DSS, SAS 70, Record Retention, and Business Process Improvement reviews   Performed investigations of internal fraud or presumptive fraud with a view to gathering evidence that could be presented in a court of law   Coordinated and perform compliance audits in accordance to the information protection, data asset and threat provisions under the Gramm-Leach-Bliley and Sarbanes-Oxley Acts.   Coordinate with Incident Response teams for post-event diagnosis, investigation and documentation.   Evaluated and assess implementation of the disaster recovery/business continuity plan   Provided effective project (audit) guidance and leadership to team members and management as it relates to data security and industry compliance Education MBA Howard University - Washington, DC BS in Certified Information Security Manager University of the District of Columbia Skills DATABASE (6 years), SOLARIS (3 years), UNIX (3 years), UNIX SHELL (6 years), .NET (Less than 1 year), JAVA (Less than 1 year) Additional Information Technical Skills Operating Systems: Windows 2008/2012, Linux, HPUX, Sun Solaris Tools: SharePoint, Microsoft Visual Studio, TFS, Microsoft Office, LoadRunner 12.53 Enterprise. Database: SQL Server2012, Oracle9i 10g, 11g, & 12C Programming Languages: SQL, Java, Unix shell, C, JSON

Name: Daniel Hess

Email: alejandrowaters@example.net

Phone: (394)587-5270