Systems Security Analyst Systems Security Analyst Germantown, MD To be an Information Systems Security Officer or Certification & Accreditation officer for growth-oriented Information Systems Security team in organization whose focus is on systems security evaluation, certification & accreditation, systems security monitoring and auditing, risk management and assessment, information technology control, environment testing and verification and testing of IT internal controls - Sarbanes-Oxley 404 compliance. Work Experience Systems Security Analyst September 2013 to Present Responsible for coordinating and guiding system owners and security system administrators through the C&A process and multi-tasked where multiple projects ran parallel ? Identified security controls types for system using NIST SP 800 60 as a guide ? I participated in Categorizing of controls using FIPS 199 as a guideline ? Followed NIST SP 800 53 guidelines to ensure operational, managerial, & technical controls for securing sensitive security systems/ IT systems are in place ? Engaged in Implementation of selected controls using NIST SP 800 53 Appendix F ? Used FIPS 200 to define minimum security control baseline for info and information system ? Involved in performing Configuration Management and Control using NIST SP 800 128 ? Ensured the system's recoverability as define in the system security requirements by performing contingency plan test and training using NIST SP 800 34 as a guide ? Assessed program and security controls using NIST SP 800 53A as a guide to provide information necessary to determine their overall effectiveness ? Developed and maintained C&A documentations - SSPs, CPs, Risk Assessment Reports and evaluation of existing documentations for accuracy using NIST SP 800 53, SP 800 53A, SP 800 53 Appendix F, SP 800 34, SP 800 39 respectively ? Created POA&Ms and developed required mitigation strategies ? Developed and implement penetration testing and procedures ? Took the system through full accreditation by meeting all the necessary documentations and procedural requirements for the certification and accreditation of an information security system ? Worked with C&A team members, senior executives to establish and define programs, risks, and resources IT Security Analyst FIA Info Systems September 2010 to September 2013 Conducted system risk assessment and documentation of key controls using NIST SP 800 39 as a guide ? Developed audit plan and performed system controls testing and assessment of

information security using NIST SP 800 115 and business continuity planning using NIST SP 800 34 as a guide ? Evaluated current auditing procedures and proposed needed changes ? Guided system administrators and system owners through the certification and accreditation process using NIST SP 800 37 ? Ensured that procedural steps are taken implementing IT systems security requirement throughout system life cycle using NIST SP 800 64 ? Performed IT operating effectiveness test in security and operations areas ? Develop and reviewed System Security Plan by NIST SP 800 18 guidelines ? Involved in planning, and preparation for contingency and disaster recovery operations and Business Impact Analysis (BIA) using NIST SP 800 34 ? Ensured management, operation, and technical controls to secure sensitive security system are in place according to NIST SP 800 53 guidelines ? Assessment of security controls using NIST SP 800 53A to receive System Security Authorization ? Involved in continuous monitoring of security control procedures using NIST 800 137, SP 800 128 and SP 800 39 as a guide ? Involved in System Penetration testing and procedures ? Worked in self-motivated environment with strict project deadlines ? Involved in security team meetings for implementing IT system security requirements IT Auditor Core IT System Solutions September 2009 to September 2011 Performed IT system inventory ? Trained and advised IT system administrators on SOX/FISMS 404 compliance and control activities ? Analyzed policy, regulatory, and resource and procedures ? Identified internal control processes ? Analyzed processes and suggested system improvements ? Used SOX/FISMA initiative to monitor team - separation of duty log, changes in financial activities log, database query and response log, normal and unusual activities log, and scope/breath of activities log ? Participated in SOX 404 compliance framework sessions ? Verified and validated SAP ERP(Oracle) end-user security with FISMA 2002 compliance ? Performed SAP auditing to maintain consistency with policies and procedures ? Interacted with super users to ensures accuracy in account management control procedures ? Provided tracking and reporting of SOX issues remediation ? Review logs and provided documentation guidelines ? Generated SAS 70 report ? Review testing methodology for manual and automated controls Education BBA in Corporate Finance Zicklin School of Business, Baruch College 2002 Additional Information Skills: Risk

Management Policies and Procedures, Risk Management & Assessment, Security Control Categorization, Selection of Technical, Operational and Management Controls Security Plan Development and Management, Configuration Management, Privacy Assessment, Threat and Vulnerability Control and Management, Contingency Planning, Business Impact Analysis, Risk Assessment Report, Security Control Assessment, Security Assessment Report, Plan Of Action & Milestones (POA&M), Security Assessment Plan, Incident Response, Intrusion Detection System, Account Management

Name: Lindsay Davis

Email: vegavincent@example.org

Phone: 807.673.8297