Cybersecurity Consultant (GSA) Cybersecurity Consultant (GSA) Cybersecurity Consultant (GSA) - Forever Solutions Group Frederick, MD Work Experience Cybersecurity Consultant (GSA) Forever Solutions Group - Vienna, VA Present Assist System Owners and ISSOs in preparing certification and Accreditation package for the Agency's IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53rev4 Conduct security control assessments to assess the adequacy of management, operational, privacy, and technical security controls implemented. Security Assessment Reports (SAR) are developed detailing the results of the assessment along with plan of action and milestones (POA&M) Develop risk assessment reports. This report identifies threats and vulnerabilities applicable to assigned systems. In addition, it also evaluates the likelihood that vulnerability can be exploited, assesses the impact associated with these threats and vulnerabilities, and identifies the overall risk level Responsible for the development of security control test plan and in-depth security assessment of information systems in order to maintain FISMA and FEDRAMP compliance by implementing guidelines and standards identified in the National Institute of Standard and Technology (NIST) 800-53A Develop compliance reports documenting audit findings and corrective actions. Provide ISSO with composite reports detailing audit findings and recommendations to correct identified vulnerabilities Conduct I.T controls risk assessments that includes reviewing organizational policies, standards and procedures and provide advice on their adequacy, accuracy and compliance with FISMA and FEDRAMP Support the FISMA compliance program by reviewing evidence of compliance, driving necessary system and process improvements and ensure the completion of the annual compliance reports Collaborate with peers across the organization to share solutions and best practices Cybersecurity Consultant Forever Solutions Group - Beaver Valley, PA July 2017 to December 2017 Participated in daily Technical call meetings Conducted security assessments to test the security controls of Critical Digital Assets (CDAs) and determine the overall effectiveness of their controls. Worked with the Technical Team to determine security control requirements for the CDAs Conducted walkdowns of critical digital assets to determine their risk level and safety. Provided security consulting and advisory services to business units and project teams to ensure best security practices are adhered to. Facilitated Security and Safety Awareness Training Programs Reviewed Nuclear Regulatory Commission (NRC) Security guidance 08-09 and 13-10 to determine CDAs capabilities and their threat vectors. Developed and reviewed security related Policies and Standard Operating Procedures (SOPs). Worked with engineers to provide risk mitigation recommendations. Provided Subject Matter Expert (SME) advisory on security related issues. Provided information assurance to ensure all security requirements are met throughout the infrastructure setup IT Security Analyst (CMS) Forever Solutions Group - Laurel, MD September 2015 to July 2017 Assisted Business Owners and ISSOs in preparing Security Assessment and Authorization (SA&A) packages for systems, ensuring management, operational and technical security controls are adhered to a formal and well-established security requirement authorized by NIST SP 800-53rev4 Provided support to external audit teams as required (Help with gathering/presentation of evidence to validate controls effectiveness and efficiency) Analyzed/reviewed and updated System Security Plan (SSP) and Information System Risk Assessment (ISRA) Conducted follow up meetings to assist Business Owners to close/remediate POA&M items through the Remedy ticketing system Created and reviewed Privacy Impact Analysis (PIA) artifacts. This involved working closely with the Information System Security Officers (ISSOs), system administrators, application developers, and the Privacy Act Officer Conducted Security Impact Analysis (SIA) for any change or upgrade to the system (This involved working closely with application developers and the Infrastructure team). The result of the SIA documents possible change(s) to the system and an affected NIST control Updated security controls implementation status within CMS FISMA reporting tool (CFACTS) to generate a comprehensive SSP Provided security consulting and advisory services to business units and project teams to ensure best security practices are adhered to. Assisted in communicating requirements for security risk assessments for applications within the CMS Network Worked closely with the Security Operation Team to conduct internal security assessment (Identified weaknesses from vulnerability scans are remediated in accordance with defined time frames) Provided expert security guidance on IT projects such as deployment of new systems, major system upgrade, and system migration Reviewed/updated Contingency Plans to satisfy NIST annual requirement and ensure it is well documented Involved in conducting annual table top exercises to review and test the processes and procedures that would be used when real disaster occurs Provided Subject Matter Expert (SME) to support security control testing, or other form of system testing as requested by Business Owners to identify vulnerabilities in security features of an application, system, network or operational weaknesses in process or technical countermeasures Provided support to the external audit teams as required (Helped in the gathering/presentation of evidence to validate controls effectiveness and efficiency) Assisted Business Owners and ISSOs in preparing certification and Accreditation package for systems to renew an existing ATO IT Security Analyst Blue Canopy - Reston, VA August 2013 to September 2015 Provided Subject Matter Expert (SME) support on security control testing, or other form of system testing as requested by Business/System Owners to identify vulnerabilities in security features of an application, system, network or operational weaknesses in process or technical countermeasures Evaluated, maintained, and communicated the risk posture of each system to executive leadership and make risk-based recommendations to the Chief Information Security Officer (CISO) Prepared written responses to routine security and compliance inquiries by preparing, modifying documents including correspondence, reports, drafts, memos and emails Provided development guidance and assisted in the identification, implementation, and maintenance of compliance policies, procedures and work instructions Provided guidance to stakeholders on required actions (systems planning and development projects), potential strategies, and best practices for closure of identified weaknesses Created and maintained security metrics key risk indicators to help senior management to make critical security risk decisions Supported both internal and external audit activities including records collection, coordinating with other departments to collate all relevant information Participated in kick-off meetings with management and client and provided input on the System Security Plan Project Developed/created system security plan to provide an overview of Federal Information System security requirements and described the controls in place or planned to be implemented Interviewed system owner and reviewed existing system documentations to define specific, measurable, relevant and theoretically sound audit objectives Worked effectively with all levels of management, staff and cross-functional security teams within the organization to identify and implement information assurance controls authorized by NIST SP 800-53 Reviewed/analyzed artifacts to gather relevant information in the system security plan Participated in a team weekly meeting to discuss the status of the System security plan. This also served as information gathering for control implementation description requirement for the system security plan. Assisted System Owners and ISSOs in preparing certification and Accreditation package for systems, making sure that management, operational and technical security controls adhered to a formal and well-established security requirement authorized by NIST SP 800-53rev4 Conducted security control assessments to assess the adequacy of management, operational, privacy, and technical security controls implemented. Developed risk assessment reports. This report identified threats and vulnerabilities applicable to assigned systems. In addition, it also evaluated the likelihood that vulnerability can be exploited, assessed the impact associated with these threats and vulnerabilities, and identified the overall risk level Participated in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the Information System Security Officers (ISSOs), the System Owner, the Information Owners and the Privacy Act Officer Developed E-Authentication reports following NIST SP 800-63 requirements to provide technical guidance in the implementation of electronic authentication (e-authentication) Provided an independent and objective review of system documentation to ensure the documents met all requirements needed for an ATO Provided the system owner and ISSO with industry best practices and recommendations surrounding the system's security posture leading to attainment of an ATO Validated that vendors followed all relevant policies and procedures for new system set up as well as providing information assurance services on all key tasks, steps, and documentation throughout an entire decommissioning process. FISMA/C&A Analyst SmartThink March 2010 to August 2013 Designed and performed IT and infrastructure HIPPA audits related to information security policy, regulations, governance, and other security-related provisions and best practices Conducted related ongoing compliance monitoring activities to ensure effectiveness of implemented controls Tracked and communicated constraints, conflicts, or gaps to existing processes, as well as tracking cross-functional team remediation. Monitored and tracked best practices and emerging compliance changes/impacts for continuous improvement opportunities Supported both internal and external audit activities including records collection, coordinating with other departments to collate all relevant information Managed and coordinated audit-related activities with internal stakeholders and external auditors, and validating contractual obligations to ensure compliance Categorized internal and external audit results and communicating findings, including recommendations, to key stakeholders Analyzed and updated System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M) Assisted System Owners and ISSO in preparing certification and Accreditation package for systems, making sure that management, operational and technical security controls adhered to a formal and well-established security requirement authorized by NIST SP 800-53 Categorized systems based on SP -800-60 to select the appropriate NIST recommended control SP 800-53 Performed Vulnerability Assessment. Made sure risks were assessed, evaluated and proper actions were taken to limit their impact on the Information and Information Systems Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Responsible for the development of security control test plan and in-depth security assessment of information systems to maintain HIPAA compliance by implementing guidelines and standards identified in the National Institute of Standard and Technology (NIST) 800-66 Developed HIPAA compliance reports documenting audit findings and corrective actions. These reports were submitted to the alternate ISSO Involved in the security awareness and training of staff on HIPAA requirements as it relate to information technology Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard SOX Compliance Analyst Conducted periodic IT risk assessment and reviewed controls for any deficiencies. Deficient controls are then reported to the CISO for appropriate mitigation actions Conducted security controls assessment to ensure controls are implemented to comply with ISO standards Initiated and led information security awareness and training program to inform the employees of their roles in maintaining a matured security posture Contributed in weekly change management meetings to evaluate change requests (systems or application) that could lead to approval or denial of the requests, validated testing results from testing environments and promoted changes to production environment Conducted periodic IT risk assessment and reviewed internal controls against the ISO standard for any deficiencies. Deficient controls are then reported to the CISO for appropriate mitigation actions Examined information security accreditation request for approval and denial Examined events logs for irregularities. Identified irregularities were then reported as incidents. The incident response process was then initiated to mitigate the irregularities Involved in security incident management to mitigate or resolve events that had the potential to impact the confidentiality, availability, or integrity of information technology resources. Created and maintained security metrics to help senior management to make decisions Provided support to internal and external audit teams as required (Helped in the gathering/presentation of evidence to validate controls effectiveness and efficiency) Interviewed departmental heads and reviewed existing system documentation to define specific, measurable, agreed, relevant and theoretically sound audit objectives Education Bs in Cybersecurity University of Maryland-University College - Maryland 2012 to 2015 Bachelor of Science in Accounting Ho Polytechnic Skills Customer Service Certifications/Licenses Certified Information Systems Security Professional (CISSP) Certified Ethical Hacker (CEH) CompTIA Security+ Certified Authorization Professional (CAP) Additional Information Perform Security Assessment and Authorization (SA&A) documentation Develop, review and evaluate System Security Plan Perform comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems Develop and conduct SCA (Security Control Assessment) according to NIST SP 800-53A Familiar with NIST publication; FIPS 199, SP 800-60, SP 800-53rev4, SP -800-137 Excellent with COSO, COBIT, ISO, SSAE 16 (SOC1,2&3) and PCI DSS Frameworks Develop and update POA&Ms   Ability to multi-task, work independently and as part of a team   Strong analytical and quantitative skills   Effective interpersonal and verbal/written communication skills

Name: Eric Larson

Email: amberflores@example.net

Phone: 001-819-382-6601x99271