Sr. Security Analyst Sr. Security Analyst Sr. Security Analyst - BBA Aviation Clermont, FL Ms. Fermin Brings about 6 years of combined professional experience in the private and public sector in Information Systems Audits and Cyber Security with hands on experience in GDPR compliance and GDPR privacy. Proven ability to develop, grow, manage and measure Information Security and Privacy programs while promoting a culture of leadership, information assurance and compliance enterprise-wide. Experience on project management and building SOW (statement of works) for various projects, Risk Management Framework (RMF), core expertise in Cyber Security, Risk Management, Testing, FISMA, ST&E,POAMs, Security Assessment & Authorization (SA&A), Audit Engagements and ISO, and Hippa, PIA, PII, Sox 404, PCI, FedRamp. Pamela also has experience in various frameworks (COSO, COBIT, ISO27001 and well acquainted with the NIST SP 800 Series. Work Experience Sr. Security Analyst BBA Aviation January 2018 to Present Conducted risk assessment, communicate the results to management, and track the results and issues until resolution. ? Managed the Privacy Impact Assessment (PIA) lifecycle from receipt to closure, including tracking and reporting. ? Create, publish, and manage the Records of Processing Activities (ROPA) for all data processed within the purview of Information Security and the IT Group. ? Provided guidance and support to the business regarding data privacy and compliance improvements to meet US and European data protection laws. ? Analyze new system and application projects for security and data privacy implications and provide guidance to minimize privacy compliance risks. ? Evaluated Information Technology contracts, service agreements, and associated data transfer or sharing agreements for privacy and security impacts with recommendations. ? Updated and Publish Privacy and Security Policies and Standards consistent with updated General Data Protection Regulations and US privacy and data protection laws. ? Supported data identification and data flow mapping efforts to document and validate data classification and processing activities conducted across the organization. ? Maintained subject matter expertise with regard to applicable regulations pertaining specifically to information security, data privacy and Data Breach Notifications. ? Created comprehensive procedures for the 'erasure' of data subject's personal data upon request ? Builds and manages relationships with diverse

stakeholders including senior-level technical and non-technical staff. ? Ensures IT/IS policies and procedures are documented and updated according to BBA Aviation's regulatory standards, deadlines are met, approvals obtained, guidelines followed, repository usage understood, and repository / system of record up-to-date as defined by the Information Security program. ? Maintains all versions and version control for all Information Security program documentation and pipeline with a thorough understanding of the processes and communicates the status ? Delivered comprehensive awareness training for all employees on data privacy and protection. Capgemini (remote) Senior Security Consultant System Security Plan June 2017 to November 2017 Developed strategic- and technical-level policy documentation for security practitioners and network engineers administering and managing the campus networks. Provided project management support in the development of all documentation as it related to the Certification and Accreditation of the application (System Security Plan, Risk Assessment, Configuration Management Plan, and Contingency Plan) ensuring compliance with NIST 800-53a Rev4. ? GDPR-Privacy and security services- Risk assessment, Privacy Gap, Readiness and roadmap, data privacy discovery, education and awareness. Policy Writing ? Developed and maintained library of technical procedure documentation as part of larger enterprise-wide effort to enhance the capacity of the firm's information security service offerings and capabilities. ? Authoring Policies and Procedures: ? Developed Policy and Procedural documentation in accordance with NIST SP 800-40 to establish a Patch and Vulnerability Management Program, communicate risks to enterprise IT operations, define a repeatable process for identifying vulnerabilities, document security patch status, and designate a Patch and Vulnerability Group (PVG) comprised of information security practitioners and information technology engineers. IT Governance ? Proven ability to develop, grow, manage and measure Information Security and Privacy programs while promoting a culture of leadership, information assurance and compliance enterprise-wide. Authored Policies, Procedures, Standards and Guidelines: ? Developed and maintained library of policies, standards, baselines, guidelines, and procedures as part of larger enterprise-wide effort to enhance security posture ? Coordinated Cloud Deployment of Governance, Risk, and Compliance Suite: ? Installed and configured RSA

SecOps (Security Operations Management) within the RSA Archer GRC Suite ? The document also outlines GRC policy and procedures with roles for various business lines, operation teams and the compliance office. ? Installed and configured Archer RCF (RSA Connector Framework) to aggregate all actionable security alerts from Security Analytics Risk Management, Audit and Compliance ? Proven ability to swiftly assess business objectives, interact with senior leadership, assign risk ratings, make recommendations, finalize and deliver. ? Delivered data-driven strategic risk-mitigation recommendations: ? Utilized audit reports and findings as grounds for discussing measures to improve functional business processes by balancing considerations for security and ease of use ? Business process analysis and continuous improvement: Delivered multiple projects with stringent timelines for various business units as project manager and technical lead ? Led Audit Engagements: Cyber Security Analyst SMARTTHINK LLC (Contract for National Cancer Institute) - Berwyn Heights, MD December 2012 to May 2017 Performs risk analysis and security audit services, and develops analytical reports as required ? Evaluates vulnerability information, identifies false positives, documents findings, prioritizes results based on risk and provides assistance to administrators in remediation efforts ? Proactive mitigation of network and operating systems vulnerabilities and recommending compensating controls ? Supports the deployment and integration of security tools ? Analyze and recommend solutions for information security problems based on experience and security best practices for major information system products and service ? Leading the effort in developing a formal process for maintaining minor applications on an Ongoing Authorization (OA) ATO ? Conduct CDM meeting to discuss vulnerabilities and potential remediation actions with system and application owners ? Ensure identified weaknesses from vulnerabilities scans are remediated in accordance with NCI defined time frames ? Involve in NCI security awareness program to educate employees and managers on current threat and vulnerabilities ? Conduct kick off meetings in order to start security control assessment on assigned National Cancer Institute (NCI) systems ? Conduct security control assessment to assess the adequacy of management, operational privacy, and technical security controls implemented ? Develop Security Assessment Report (SAR) detailing the results of the assessment along with Plan

of Action and Milestones (POA&M) ? Conduct follow up meetings to assist information system owners to close/remediate POA&M items ? Develop System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements ? Conduct IT risk assessment to identify system threats, vulnerabilities, and risks ? Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. SMARTTHINK (contract for Federal Retirement Thrift Investment Board) - Exceeded 45% over set goal before project milestone) IT Security Analyst IT Security Analyst SMARTHINK (contract for Department of Energy) - Fairfax, VA September 2010 to November 2012 Evaluate, enhance, and support cyber security strategies, policies, standards, controls, and processes, including standards development, risk management, compliance management, and information security-related processes and procedures. ? Assess and identify security threats and risks to networks, systems, applications, etc. ? Assist in developing and implanting cyber security policies, standards and guidelines ? Develop, recommend & test security controls to meet information assurance requirements ? Define and perform security audits, evaluations, and risk assessments of complex operational data processing systems and facilities ? Utilize NIST Risk Management Framework, the critical security controls and other standards as defined by organization ? Collaborate with peers to ensure best practices are in place regarding security system integration and software development Participate in internal reviews of auditors, operational risk assessment staff, compliance/reporting staff to prepare assessments or reports of operational risks associated with infrastructure, access to system, exposure to attacks. SA &A - Columbia, MD January 2011 to September 2012 Development of SA &A process documents ? Conducting in depth review of new and existing IT systems in order to identify the appropriate mitigation strategies required to bring systems into compliance and established policy and industry guidelines ? Analyze business models, workflows of current policies, practices dimension as they relate to support of the information system ? Providing ongoing gap analysis of current policies, practices and procedures as they relate to established guidelines outlined by NIST, FISMA, etc ? Conducted kick off meetings in order to categorize FRTIB's systems

according to NIST requirements of Low, Moderate or High system ? Developed a security baseline controls and test plan that was used to assess implemented security controls ? Conducted security control assessments to assess the adequacy of management, operational privacy, and technical security controls implemented. Security Assessment Reports (SAR) were developed detailing the results of the assessment along with Plan of Action and Milestones (POA&M) ? Developed risk assessment reports. These reports identified threats and vulnerabilities applicable to FRTIB systems. In addition, it also evaluates the likelihood that vulnerabilities can be exploited, assess the impact associated with these threats and vulnerabilities, and identified the overall risk level ? Assisted in the development of an Information Security Continuous Monitoring Strategy to help FRTIB in maintaining an ongoing awareness of information security (Ensured effectiveness of all security controls) ? Led 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 Owners, the Information Owners ? Developed a system security plan to provide an overview of federal information system security requirements and described the controls in place or planned by FRTIB to meet those requirements. IT Security Analyst SMARTTHINK LLC - Washington, DC October 2008 to September 2010 Developing and updating security authorization packages in accordance with the client's requirement and compliant with FISMA. Core documents that the candidate will be responsible for are the System Security Plan, Risk Assessment Report, Security Assessment Plan and Report, Contingency Plan, Incident Response Plan, Standard Operating Procedures, Plan of Actions and Milestones, Remediation Plans, Configuration Management Plan ? Develop and maintain the Plan of Action and Milestones and support remediation activities. ? Validate that protective measures for physical security are in place to support the systems security requirements. ? Maintaining an inventory of hardware and software for the information system. ? Developing, coordinating, testing and training on Contingency Plans and Incident Response Plans. ? Perform risk analyses to determine cost-effective and essential safeguards. ? Support Incident Response and Contingency activities ? Able to perform security control assessment in using NIST 800-53A guidance ? Conduct Independent scans of the

application, network and database (where required) ? Provide continuous monitoring to enforce client security policy and procedures and create processes that will provide oversight into the following activities for the system owner. Education BA Kaplan University BA of Science in Cyber Security Technology Present Skills SECURITY (9 years), NIST (6 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (3 years), FISMA (3 years), AUTHENTICATION (Less than 1 year) Additional Information TECHNICAL SUMMARY/ SOFTWARE, TOOLS ? GDPR, Privacy Gap assessment, Data privacy discovery, FIPS, FISMA, HIPAA, Security Assessment & Authorization (SA&A), SCAP, OMB Circular A-130 Appendix III, NIST 800-53A Rev 4, COSO, SAS-70/SSAE-16, ISO 27001,Windows,C-Facts,IFISMA,Microsoft Word, Excel, FIPS 199, TCP/IP & Networking Protocols, Wireshark Packet Analysis, Group Policy Management, Linuxm E-Authentication ,PTA, PIA, RA, ST&E, POA&M, SP 800-53A Rev 4,SP 800-30,SP 800-37, SP 800-66. QUALIFICATIONS & SKILLS ? Prioritizes business strategic objectives to make informed risk decisions ? Independently researches complex problems, asks/answers questions, meets deadlines, finalizes, and delivers ? Analyzes technical reports for statistics and trends, synthesizes large amounts of data, composes presentations, technical reports, and business correspondence

Name: Lisa Garcia

Email: devin69@example.com

Phone: +1-724-361-1873x34502