IT Security/Business Analyst IT Security/Business Analyst IT Security/Business Analyst - GAMA-1 Technologies, Inc Laurel, MD for Growth Seeking to be engaged as an Information Security Engineer or Information System Auditor in a growth- oriented environment where my skills and specialties in System Security Monitoring, Risk Assessment, System Audit Engineering, FISMA, Sarbanes-Oxley, Testing of Information Technology Controls and Developing Security Policies, Procedures and Guidelines, can be put into maximum use. Also seeks engagement in an environment where building new customer relationships and deepening existing ones through the provision of system assistance to help users to take full advantage of Information Technology (IT) needs for their daily operations in a secure environment. Software Platforms and System/Network Scanning Tools CSAM, UNIX, Windows, LAN/WAN, LDAP, Wireless Network, TCP/IP, Remedy, DMZ, IPS/IDS, Cisco Routers/Switches, ArcSight, RSA Archer/eGRC, Oracle, PGD, DISA, SRR, Eye Retina Scan, SAINT,IBM AppScan, Tenable Security Center, Big fix, RSA, C++, C, Java, Microsoft Word, Excel, Project, Access, Power Point, Publisher, Visio, SharePoint, SIEM Tools such as LogRhythm, Nessus Vulnerability Management, and QRadar detections. Knowledge and experience using Nessus Vulnerability Management tools to manage a network through log analysis and recommending the right action for system remediation. Knowledge of financial industry governance, risk management, and compliance regulatory processes Knowledge and experience in the entire RMF process and its compliance using NIST publications and standards Knowledge of GRC, UTM, IDS/IPD tools of different kinds to ensure effective system security and compliance Compliance/Policy and Procedure scripting and cross-referencing using Enterprise Issue Management (ESM), Enterprise Risk Management (ERM)/COSO/COBIT procedures as well as ISO 27001:2013 standards Standards and Frameworks COSO/COBIT, Sarbanes-Oxley Act, SAS-70/SSAE 16 , ITIL, ISO 27001, Privacy Act of 1974, Gramm-Leach-Bliley Act (GLB), HITECH/HIPAA, Security Assessment & Authorization (SA&A), OMB Circular A-130 Appendix III, FIPS 199, NIST 800-53, NIST 800-60 rev I Vol II, NSA Guide, STIG, DoD 8500.2, DITSCAP, DoD 8510.bb, DIACAP, FISMA, FISCAM, Security Content Automation Protocol (SCAP), the FedRAMP framework and Cloud services like SaaS, PaaS, and IaaS. My specialized areas of frameworks

include IT Governance, Controls, Objectives, Rules of Engagement, Administering Procedures & Reporting, Monitoring and Compliance, engaging with Stakeholders while working within the governance frameworks such as COBIT, ISO, NIST. Authorized to work in the US for any employer Work Experience IT Security/Business Analyst GAMA-1 Technologies, Inc September 2016 to Present Role/Duty: - Lead FISMA Risk Management and System Security Monitoring, System Audit Engineering and log analysis based on NIST compliance requirements. - Lead CSAM tool administration, IT security control assessment, technical documentation and management, on the status of IT security risk assessments and implementation of NIST developed IT security control standards and policies. - System Security Monitoring and status reporting - Using CSAM as a centralized tool for POA&M management including creating, tracking, and timely closing, as well as automating system inventory and FISMA reporting capabilities. Conducting the RMF process to categorize system, select and implement appropriate controls for system security against CIA - Supporting and reporting on Contingency Planning and Disaster Recovery process. - Supporting Nessus vulnerability log analysis and reporting on threats and associated impacts for proper control management to leverage system security. - Supporting data sharing procedures and Interconnection Security Agreement documentation. Data Security Analyst Maine Department of Labor/vTech Solutions, Inc August 2015 to September 2016 Role/Duty: - Acting as the main system data security analyst for a new project to ensure compliance with NIST Standards. - Leading a team of security personnel in CSAM) tool IT security assessment, documentation, management, and reporting on the status of IT security risk assessments and implementation of NIST developed IT security control standards and policies. - Using CSAM as a centralized tool for the management of POA&M including creating, tracking, and closing, as well as automating system inventory and FISMA reporting capabilities. Conducting the RMF process to categorize system, select and implement appropriate controls for system security against CIA - Using System/Network scans and other vulnerability tools, and generating reports as part of risk assessment process to identify system vulnerabilities, threats, and associated impacts in order to effect proper controls and ensure system security. - Assist system programmer in designing data governance procedures for system

- Engaging data sharing partners in data field definition and efficient system security discussions Information Security Analyst (Lead) Smarthink Limited - New York, NY June 2014 to August 2015 Role/Duty: - Using and analyzing vulnerability scanners such as IBM AppScan, Saint, and 3 Tenable Security among others to ensure network and application security - Led a team in HIPAA Compliant Cloud Service Patient Data Security in New York - Assisted in establishing a HIPAA disaster recovery/contingency plan for new Patient Data machine in New York - Team Member in HIPAA Compliant system categorization in Baltimore - Auditing system security installations to ensure the Confidentiality, Integrity and Availability (CIA) of system and compliance. - Conducting continuous system monitoring to avoid potential future vulnerabilities and threats - Using UTM methods such as IDS/IPS to help analyze DMZ Firewall configurations for effective system security and ensuring control effectiveness - 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 - Drafting Contingency Plan recommendations for system owners - Provide expert technical security guidance on IT projects such as deployment of new systems, major system upgrade, and system migration Assistant Information Security Analyst Smart-Think Limited January 2010 to May 2014 Role/Duty: - Assist the Senior Information Security Officer in the conduct of Information Security assurance roles and ensuring system safety. - 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) - Assisted in the development of rules of engagement documentation in order to facilitate the scanning of FRTIB network, applications and databases for vulnerabilities - Developed Risk Assessment Reports (RARs) that addressed identified system threats and vulnerabilities, and recommending timely appropriate and actionable solutions to ensure information safety. Assisted in the development of Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA).

Education Master of Science in Finance and Information Systems University of Maryland University College, College Park February 2016 Masters in International Criminal Law in International Criminal Law University of Sussex February 2006 Bachelor of Science in Economics and Law University of Science and Technology 2002

Name: Sara Camacho

Email: geralddavis@example.net

Phone: (477)607-8522