SR. Audit Consultant SR. Audit Consultant SR. Audit Consultant Clarksburg, MD Seeking an Information System Auditor or Information Compliance position in a growth-oriented organization with focus on Shared Assessment, FISMA, Sarbanes-Oxley 404, Cloud based Solutions, Implementation and Big Data Management ISO 27001 system security monitoring and auditing; risk assessments; audit engagements, testing information technology controls and developing security policies, procedures and guidelines, DLP. STANDARDS Shared Assessment, COSO/COBIT, Sarbanes-Oxley Act, SAS-70/SSAE16, ITIL, ISO 27001, ISO 27002 Privacy Act of 1974 ,Gramm-Leach-Bliley Act (GLB),Certification and Accreditation, Project Management, Change Management, OMB Circular A-130 Appendix III, NIST 800-53,FIPS, FISMA, FISCAM, GRC TOOLS Work Experience SR. Audit Consultant ComScore Reston, Virginia - San Antonio, TX November 2018 to March 2019 USAA Fredericksburg, San Antonio, TX Sensitive Data Management Lead December Writes basic Information Security governance. Publishes, maintains, and interprets moderately complex Information Security governance (e.g. policies, principles, standards). Executes repeatable methods and measurements to determine Information Security risk and recommends improvements to the process. Performs security risk assessments of moderately complex projects, new technologies, business partners, and third parties. Integrates risk management strategies and educates and consults with risk owners on best practices. Provides consulting (advice, guidance and assistance) to individuals and teams on Information Security risk, to guide the security direction of USAA development projects and departmental initiatives. Determines requirements, recommends system security configurations, DLP Implementation and risk mitigation effectiveness. Responds both verbally and in writing to routine inquiries and periodic exams from both internal control partners (e.g. legal, compliance, audit, risk) and external control partners (e.g. regulators, external auditors, third-parties). Guides and assists process owners in the identification, development, and testing of Information Security controls for risk mitigation effectiveness. ComScore Reston, Virginia- SR. Audit Consultant, (Nov 2018-March 2019) Conducting of application security and development process that includes specification documents, new functionality, test scenarios, and processes and reviewing ComScore clients SDLC processes including test case scenarios, change management, Incidence Management, and Vendor Quality Management to ensure that there is existing evidentiary documents that demonstrate compliance with policies and procedures with those provided by clients. Testing all developments and new requirements for bugs, evolution of the product before pushing into production and conformance in GxP systems. Managing lifecycle of complex cross-functional IT Audit functions across. Evangelizing AWS services and their relevance to enterprise level data problems while focusing on building petabyte scale big data digital measurement solutions in Advertisement Technology and Digital Measurement Leading Dev Ops teams preparing for Cloud migration from On Premise Data Centers to AWS Cloud Setting up ComScore first Enterprise Program & Portfolio Management practice focusing on data governance and compliance functions on a Cloud based infrastructure. Creating Identity & Access Management best practices, Data Supply Chain processes and Access Rights Management. Vendor Risk Assessment Team Lead FreddieMac, Maclean, Virginia March 2018 to November 2018 Help define Role-based access control (RBAC) by regulating access to systems, resources based on the roles of individual users within the enterprise to enable individual users to perform specific task, such as view, create, or modify a file. Lead in the development and enforcement of organizational policies leading the overall organizational Engagement with client stakeholders to effectively instill the relevance and importance of the vendor Risk management program. Authorize and set program priorities, initiate change orders as required during the maturation of the program, advise on personnel decisions, and make non-revenue impacting binding agreements with the client in the interests of furthering the efficiency of the overall vendor risk assessment effort. Supervise the organization assessment team (onsite and remote), assigning work effort and prioritizing within the framework of agreements, SLAs and emerging actions. Execute vendor risk assessments. Review, create and rewrite policies, control standards and procedures. Coordinate implementation, and changes with policy control owners. Create and update documentation, procedures and training materials to ensure consistency with new and newly rewritten control standards and procedures Provide quality assurance oversight to assessors' work product. Provides reports and briefings as client determines. Approve and present recommendations to the client on program enhancements. Produce and maintain all status reports associated with the program-real time. Prepare KPI status reports as agreed to by the client. Create, communicate and present status reports and brief senior management and client as required. I.T Security Technical Lead UPS-Mahwah - Mahwah, NJ September 2015 to March 2018 Helps develop the Shared assessment program, and conducts annual vendor risk assessment compliance program. Leads Vendor Risk Assessment Planning & Scheduling, Vendor reconnaissance and updates with owners. Helps with Questionnaire review, updates, and initiation. Manage offshore resource(s), activities, results, and track program metrics. Manages Vendor interactions and Issues and also report to upper management. Conducts high Risk Vendor Assessments and Interactions for both onsite and offsite. Conducts Process Improvement matrix. Advise client on VRM Best Practices Alignments and prepare Weekly, Quarterly, Ad-Hoc Reporting. in-depth understanding of Sarbanes Oxley Section 404 and SSAE 16 SOC reporting. Experience with general Information Technology controls design and reviews. Strong knowledge of IT audit methodologies and control frameworks of IT platforms, processes, systems and controls, including areas such as logical access, physical security, and change management controls at an infrastructure and application level. Oversees ongoing activities related to development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, information in compliance with federal and state laws and the information privacy practices. Perform initial and periodic privacy risk assessment and conducts related ongoing compliance monitoring activities with coordination with the entity's other compliance and operational assessment functions. Security Consultant (ISO Auditor) SR.IT November 2014 to August 2015 M3USA, Pennsylvania) Protect M3USAsystem by defining access privileges, control structures, and resources, Control testing and identifying findings and reporting violations to management. Upgrade IT operations by implementing and maintaining security controls. Participate in strategic and operational governance processes of the business organization while assisting the promotion of IT solutions and services. Develops audit objectives for the conduct of IT audits. Prepare, review audit programs necessary to fulfill the audit objectives. Assists with Department's risk assessment and audit plan development process. Conducts and lead

IT audit process to include engagement planning, coordination, scope determination, risk program, procedures, testing, and evaluation of results. Prepares adequate documentation (work papers) supporting all audit work performed to support the preparation of a written report to Management Prepares comprehensive, well-written Internal Audit Reports summarizing the review results. Follows-up on status of prior IT audit recommendations to ensure that report recommendations are implemented on a timely basis. Provides support to the IT Manager, Finance Manager, Internal Control Staff, External Auditors, and to Management with respect to information technology and its application to the business. Takes direction from Head of IT and the Head of Internal Audit to perform those duties that may be assigned from time to time. Understanding of internal control concepts and experience in applying them to perform, manage and report on the evaluation of the business processes, areas, functions. Strong verbal and written communication skills to peers, and business management presentation Security Auditor SR.IT - Chicago, IL January 2014 to September 2014 Chicago) Responsibilities: Lead implementation of ISO 27001-27002 controls to achieve ISO 27001:2016 certifications including the implementation of information security management system (ISMS). Responsible for writing and documenting guide wire policies and procedures and audit evidence of compliance in preparation of certification audit. IT Security Analyst Quotient-Inc January 2012 to December 2013 on contract with National Assessment Governing Board (NAGB) Conducted a kick off meeting in order to categorize NAGB'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 a security control assessment to assess the adequacy of management, operational privacy, and technical security controls implemented. A Security Assessment Report (SAR) was 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 NAGB network, applications and databases for vulnerabilities Developed a risk assessment report. This report identified threats and vulnerabilities applicable to NAGB systems. In addition, it also evaluates the likelihood that vulnerability can be exploited, assesses 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 NAGB in maintaining an ongoing awareness of information security (Ensure continued effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions Led in the development and implementation of Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA) by working closely with the Information Owners and System Owners. Developed an E-Authentication report to provide technical guidance in the implementation of Electronic authentication (e-authentication) Developed a system security plan to provide an overview of federal information system security requirements and describe the controls in place or planned by NAGB to meet those requirements. Ensure availability, scalability, uptime & security requirements of SaaS Services and systems are clearly understood and addressed to preserve the integrity and design of the Security system to support mission-critical infrastructure necessary for business operations. Information security officer Cyber Elites Technologies, Maryland March 2006 to December 2011 Conducted periodic IT risk assessment and reviewed IA controls for any deficiencies. Deficient controls are then reported to the ISSO for appropriate mitigation actions Conducted security controls assessment to ensure controls are implemented to comply with ISO 27001 and 27002 standards Initiated and led information security awareness and training program in order to inform the employees of their roles in maintaining a mature security posture Contributed in weekly change management meetings in order to evaluate change requests (systems or application) that can lead to approval or denial of the requests, validated testing results from testing environments and promote changes to production environment Examined information security accreditation request for approval and denial base Examined events logs for irregularities Identified irregularities are then reported as incidents to management. The incident response process is then initiated to mitigate these irregularities Involved in security incident management in order to mitigate or resolve events that have the potential to impact the confidentiality, availability, and integrity of information technology resources. Created and maintained security metrics in order to help senior management to make decision Involved in third party contract evaluation in order to award contract in to the most cost effective bidder Provide support to internal and external audit teams as required Perform audits on financial systems using FISCAM Ensure availability, scalability, uptime & security requirements of SaaS Services and systems are clearly understood and addressed. Preserve the integrity and design of the Security system to support mission-critical infrastructure necessary for business operations. Under minimal supervision, Produce deliverables in alignment with overall Transformation program demonstrating mastery skills in area of sub specialization. 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) 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. 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 continued 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 and the Privacy Act Officer Developed an E-Authentication report to provide technical guidance in the implementation of electronic authentication 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 requirement Computer Lab Monitor Montgomery College February 2005 to January 2006 Assisted Students with PC and Desktop Application Issues Regularly performed hardware and Software maintenance Facilitated a weekly one-hour seminar on how to use Microsoft Office

Applications. Engaged and tracked Priority issues with responsibility for the timely documentation, and escalation PROFESIONAL AFFILIATION Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA) (ISC) 2 Transcend Technology Shared Assessment International Standard Organization Education Bachelor of Science in Cyber Security University of Maryland, College Park - College Park, MD Bachelor of Science in Statistics Ho Polytechnic University Additional Information I am specialized in areas such as Cyber security, Information Assurance (IA), Certification and Accreditation (C&A), Risk Management, Authentication & Access Control, System Monitoring, Regulatory Compliance, Physical and environmental security, Passion for Cloud technologies with in-depth knowledge of public and hybrid cloud platforms, Expertise in creating, executing & implementing Enterprise Cloud solutions, Data Governance and Data Strategy implementing adoption of Cloud Best Practices, Audit frameworks and IT Standards (COBIT, ITIL) ISO 27001 Security Management Controls SOC 1 Audit Controls Report, SOC 2 & SOC 3 Security, Availability, & Confidentiality Report. Project Management, Incident Response, and Disaster Recovery. I possess a strong managerial skill, excellent in relation building and developing strategic partnership. I am an expert in FISMA, FEDRAMP, and Shared Assessment compliance, Security Training, developing security policies, procedures and guidelines. I am highly adaptive and have superior analytical and organizational skills as well as familiar with a wide variety of applications, databases, operating systems and network devices. I am a fast learner, have the ability to multi-task, and can also work independently and as a contributing team member. I have a strong verbal/written communication skills and Technical Writing skills. I have 10+years of experience in information security; with nine of those years spent in the IT audits experience. My mission professionally is to help organizations identify, threat and manage information risks. Typically, I assist organization define their IT/IS strategy, aligning overall business strategy to IT/IS strategy, identifying business/technology risks and putting in place appropriate controls to manage the risks, managing IT/IS programs and operations.

Name: Gregory Mejia

Email: gregory72@example.net

Phone: 001-252-582-9036x9796