Lucy Martey,

**Phone Number: 512-905-2173 Email:** [**marteyl85@gmail.com**](mailto:marteyl85@gmail.com)

**Round Rock, TX 78664**

# Personal Objective

A Certified Information Security Manager with thorough knowledge and understanding of security policies and compliance in accordance with FISMA, FISCAM, NIST, HIPAA, OMB, and PCI directives, guidance, and processes. I have experience in working on FISMA, NIST 800-37 Risk Management Framework (RMF), Vendor Management, POA&M Management, creating security artifacts, and Continuous Monitoring of security systems and help protect the information systems and as Information Assurance.

## Education

Austin Community College-

## Oracle Database

Western Governors University

Bachelors - Cybersecurity

## Certification

CompTIA Security +

Oracle Database

## Skills Set Summary

* Introduction to SQL
* Risk Vision
* MS Projects (Advanced)
* MS Excel (Advanced)
* ITIL
* Risk Management Framework
* NIST SP 800 series including SP 800-53, SP-800-53A, SP 800-60, SP 800-61

# Professional Experience

## Workforce Solutions, San Antonio TX

## Senior Information Security Consultant January 2020 to Date

* Maintain system certification packages in centralized repository, supporting primarily NIST 800-53, and Risk Management Framework, Continuous Monitoring and Risk Scoring (CMRS), and DoD Information Technology (IT) Portfolio Repository (DITPR).
* Manage Plans of Action and Milestones (POA&Ms) and System Controls within centralized repository.
* Perform cybersecurity gap analyses between client implementations and requirements articulated in cybersecurity frameworks and best practices.
* Create artifacts to support making accreditation decisions to include System Security Plans (SSPs), control matrices, security assessment reports, and Plans of Action & Milestones (POA&Ms).
* Develop, review, and critique assessment and authorization (A&A) documentation in compliance with DoD Cybersecurity policy and agency guidance, including DoD, ICD, CNSS, and NIST special publications.
* Review Tenable Nessus vulnerability and compliance scans and Web Inspect application scans as part of security control assessments. Results were used to validate the effectiveness of security controls and also presented as part of the assessment report package.
* Research security standards/tools; review or conduct system security and vulnerability assessments of cloud and on-prem environments in a fast-paced, demanding environment.
* Develop, maintain, and evaluate security documentation, including System Security Plan, System Security Authorization Agreements, COOPs, and SOPs.
* Independently review security artifacts provided by program offices and other organizations and assess both the technical and functional adequacy of the cybersecurity/information assurance controls.
* Continually evaluating system security posture and make recommendations to Senior staff for correction and implementation plans.
* Assists in the development of NIST / FISMA SA&A documentation for systems and networks undergoing certification and validate the quality of deliverables produced by the team
* Assess risks, identify mitigation requirements and develop accreditation recommendations; be responsible for tracking SA&A requirements for assigned systems and validate that task are on schedule, and ensure the delivery of quality documentation
* Assist in the creation of Security Authorization Packages (SAP) with the responsibility for gathering information from system owners, applying data to the appropriate templates, and attending meetings in support of the effort
* Assist in conducting tests of IA safeguards in accordance with test plans; perform system audits to assess security related factors for systems

**Farmers Insurance, Austin, TX**

**Information Security Risk Analyst June 2015 – Dec 2019**

* Perform security control test plans and conduct in-depth security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and polices safeguards in order to maintain HIPAA compliance base on Office of Civil Right (OCR) protocol, NIST SP 800-66 Rev1 and security controls (NIST SP 800-53)
* Conducted Contingency Plan tests using the tabletop and/or functional method at least annually and updated the plan. These tests were conducted with members of application teams that have been identified as having a part to play when it comes to system resumption activities. Results were discussed during the “Lessons Learned” phase and factored into future contingency planning activities
* Managed all information systems assurance and accreditation materials maintained with the Cybersecurity governance, risk, and compliance ( GRC) Tools.
* Maintain information systems assurance and accreditation materials for all efforts relating to the third-party risk management that keep the program in line with best practices.
* Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level within the Third-party risk environment.
* Monitor and evaluate third parties’ compliance with information technology (IT) security, resilience, and dependability requirements across all capabilities using implemented capabilities.
* Use of third-party risk evaluation tools to help reduce organizational cyber risk with third parties
* Perform security reviews, identify gaps in security architecture and develop a third-party risk management plan.
* Perform risk analysis on third party capabilities (i.e. threat, vulnerability and probability of occurrence) whenever an application or system undergoes a major change.
* Communicate with IT client team to gather evidence, developed test plans, testing procedures and documented test results and exceptions
* Conduct security walkthroughs, formulated test plans, documented gaps, test results, and exceptions; and develop remediation plans for each area of testing

## Sears Holding Corp., Austin, TX

**Cybersecurity Analyst April 2013 - June 2015**

* Lead risk methodology development and execution maintain updates and mapping of governance, risk and compliance (GRC) assessments for changing requirements/criteria related to SOC1, SOC2, SOX, in addition other regulatory or industry requirements such as HITRUST, CCPA, GDPR per applicable guidelines and
* Lead risk methodology development and execution maintain updates and mapping of governance, risk and compliance (GRC) assessments for changing requirements/criteria related to SOC1, SOC2, SOX, in addition to other regulatory or industry requirements such as HITRUST, CCPA, GDPR per applicable guidelines and
* frameworks: ISO 27001:2005, NIST 800, CMMC, NIST/CSF, PCI, GDPR, HITRUST and FISMA
* Reviewed and updated Plan of Action and Milestones (POA&Ms), in agency’s Cyber Security Assessment and Management (CSAM) tool. Worked with system administrators to resolve POA&Ms, gathers artifacts and creates mitigation memos and corrective action plans to assist in the closure of POA&Ms.
* Created Waivers or Risk Acceptance Memos to assist in the effective management of system risks. These memos were created in cases where prescribed security controls could not be adequately implemented. Also identified and presented compensating controls needed to offer protection for information systems
* Conducted risk assessments, provided recommendations and engaged in remediation activities
* Monitored, reported and educated staff on HIPAA security and Privacy compliance
* Routine development of HIPAA compliance reports, documenting auditing findings and corrective actions
* Demonstrated ability to manage a privacy program in an integrated healthcare delivery system

**Spec’s, TX Oct 2011 - April 2013**

**Information Security Analyst**

* Scheduled and led kick off meetings with system owners to help identify assessment scope, system boundary, the information system’s category and attain any artifacts needed in conducting the assessment.
* Maintained information security governance, risk and compliance of activities within NIST

Risk Management Framework (RMF) to designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60

* Ensured that established internal control procedures were compliant by examining reports, records, documentation and operating practices.
* Performed continuous monitoring on asset vulnerabilities, prioritized vulnerability list and addressed critical weaknesses in the systems.
* Conducted FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations; conducted out-briefings.
* Provided Assessment, Authorization and Information Assurance support to include security test and evaluation (ST&E), security control assessment, vulnerability scanning, vulnerability assessment, POA&M management, IT security policies and procedure developments.

## 

## References: Available Upon Request