**HAZEL FREMPONG**

Phone: (914) 426-5639

Email: Lexyhaze@yahoo.com

**PROFESSIONAL SUMMARY**

Develop and maintain ATO packages, security documentation (artifacts), information system policies, SOPs, and internal training manuals.

Conduct PTA and PIA on systems in preparation for the A&A process and develop training material and presentations on privacy for training and awareness purposes.

Carry out vulnerability management in accordance with NIST, FIPS, FISMA, RMF, FedRAMP and industry best security practices.

Develop and maintain ATO Packages for information systems such as the System Security Plans (SSP), Security Assessment Reports (SAR) and Plan of Action and Milestones (POA&M).

Performed Assessment and Authorization (A&A) activities by developing and reviewing required ATO security documents that supports the implementation of RMF, identifying risks, validating the mitigation of Plans of Action and Milestones, analyzing system designs, and assisting with A&A processes that may prevent a system from receiving authorization.

Integrate information security, and risk management activities into organizational enterprise architecture, and System Development Lifecycle (SDLC), using applicable OMB, FISMA, and NIST standards.

Strong technical writing skills/ development of detailed workflow charts for ATO processes

Possess the ability and knowledge to facilitate strategic best practices in utilizing the appropriate security controls to mitigate vulnerabilities to achieve confidentiality, integrity, and availability of organizational information system.  
Strong work ethics, great team player and an uncompromising devotion to customer service delivery.

**CLEARANCE**

PUBLIC TRUST

**Work Experience**

* Develop NIST / FISMA ATO / 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 within the agency and validate tasks are on schedule, and ensure the delivery of quality documentation
* Develop, review and update System Security Plans (SSP)
* Conduct Security Control Assessments on systems up for an ATO review and renewal
* Perform vulnerability/risk analyses of Information Systems and applications during all phases of the system development life cycle
* Coordinate, develop, and evaluate security programs for the organization. Recommend information assurance/security solutions to support customers’ requirements
* Identify, report and resolve security incidents

**Dept. Veterans Affairs, DC, Washington (Vital-Edge) October 2018 – Present**

***Lead Information Assurance Analyst***

* Coordinate and facilitate ATO Decision Meetings and develop Authorizing Official System Briefing (AOSB)
* Support system stakeholders with AOSB completion and track ATO status and perform continuous monitoring analysis
* Work with stakeholders and the Privacy Office to review Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) for compliance with applicable privacy policies and regulations.
* Lead DevSecOps Policy and Procedure team and develop topics for organization training calls.
* Liaise with system stakeholders to review and update supporting security artifacts such as Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP) and MOUs/ISAs.
* Provide Plan of Action and Milestones (POA&M) support services to complete identified vulnerabilities to include tracking, updating, and managing the POA&Ms.
* Support the security A&A process by ensuring that the system support needs are met for A&A system implementation, operation & maintenance, and information system compliance.
* Host and facilitate kick-off meetings and presentations with clients on the operational security posture for the systems in their purview and on security related policies.
* Assist in the Categorization/Recategorization of system in eMASS using NIST 800-60 and FIPS 199.

***Aetna*, Rockville, MD February 2015 – November 2018**

**Support Specialist and Compliance Analyst**

* Achieve revenue, customer membership and profit earnings growth by providing strategic and technical support throughout the operation of systems support process.
* Leverage understanding of Risk Management functions to drive oversight, gap assessments, and remediation of business information systems.
* Effectively manage risk and ensure controls are operating effectively.
* Promote cross-functional efforts to deliver end to end implementation.
* Analyze and test system inputs and outputs for reasonability and functionality.
* Ensure Confidentiality, Integrity and Availability are intact.
* Provide operational support in mitigating risks in support of compliance risk management tasks.
* Review and update policies and procedures.

**Congressional Federal, Washington, DC February 2012 – February 2015**

***Cybersecurity Analyst***

* Provided operational and technical support for the processing of various meta data.
* Tested operational and transactional processes for least privilege and separation of duty.
* Provided analytical support in executing continuous monitoring processes and review and update security artifacts and documentation.
* Analyzed and defined security requirements for information protection.
* Conducted compliance audits and ensured service compliance with established security policies to reduce information and data loss and safeguard client privacy.
* Review currency transaction reports (CTR) and Suspicious Activity Reports (SARS) and ensure Bank Secrecy Act Laws are in compliance.
* Prepare and evaluate Risk Assessment Reports.
* Review, update and maintain documentation of System Test and Evaluation (STE), Configuration Management Plan Tests, PTAs, PIAs and Incident reports
* Assisted in establishing a continuous monitoring strategy to monitor and track security related defects and the status of their resolutions and make recommendations to PM.

**Best Western Hotel, Hampton, VA January2009 – December 2011**

***Auditor***

* Identified and managed risk by reviewing and assessing service processes.
* Reviewed operational procedures to assess adequacy of managerial, operational, and technical controls.
* Performed data analysis to identify vulnerabilities in order to implement countermeasures and safeguards.
* Tested operational and transactional processes for least privilege and separation of duty.
* Tested administrative controls to identify areas of inefficiency in operations.
* Reviewed audit logs to ensure accuracy and completeness.
* Perform clerical duties such as filing and storing sensitive documents that contain PII and financial data.
* Assisted in creating and reviewing of training materials.

**EDUCATION**

**Stony Brook University – Stony Brook, NY 2004 - 2008**

*Bachelor of Arts in Political Science*

**INFORMATION SECURITY CERTIFICATION**

CompTIA Security+, CISM