**LIZETTE B NAMBO**

**Cell: 859 433 4754**

**Fairfield Ohio, 45014**

**Lizettebea51@gmail.com**

**UNITED STATES CITIZEN with ability to obtain Security Clearance.**

**PROFESSIONAL SUMMARY**

* Highly- qualified **Cyber Security professional with over seven years of information Security** and information technology experience.
* Advanced understanding of the **NIST 800-53 and FedRAMP security control framework** and associated control families and requirements.
* Vulnerability Scanning and Analysis, Certification and Accreditation (C&A), Project Management, NIST 800 - 53 Rev1 and rev4 and NIST SP 800-37 rev 1, 800-18, 800-53 rev3 and 800-34, FIPS, FISMA Security Content
* Thorough understanding of **NIST 800-53 Rev 4 and 5 security controls. This includes AC, IA, AU, PE, MA, SC, CM, CP, IR, SA, SI,** etc control families.
* Automation Protocol, NIST Family of Security Control, FedRAMP Security Assessment Framework, Incident, and Contingency Planning. Testing of IT controls to ensure Confidentiality, Integrity, and Availability of the system resources. Possess strong analytical and problem-solving skills
* Knowledge of the process to obtain a system **ATO and requirements to maintain the ATO.**
* An IT professional with experience in vulnerability management, **security control implementation, assessment and authorization, POA&M management, continuous monitoring, as well as risk assessment**.

**ACTIVE CERTIFICATIONS:**

* **CompTIA Security+ Ce-**
* **Certified Information System Manager (CISM)**

**EDUCATION BACKGROUND**

• SKYTECH IT Consulting LLC, Atlanta GA **(Cybersecurity and Information Security training)** 2015

• University of Buea, Cameroon **(BSc Computer Science) –** 2011.

**TECHNICALSKILLS/STANDARDS/SOFTWARE**

NIST Guidelines Publications |Certification and Accreditation (C&A) | Assessment and Authorization (A&A) | HIPAA & PRIVACY ACT training. | IT Security Compliance | Vulnerability Assessment | Network Vulnerability Scanning | Information Assurance | System Risk Assessment | System Development

Life Cycle| Nessus Vulnerability Scanner| C-SAM| Splunk |SharePoint | Nexpose| LAN | WAN| NIST SP 800-53| SP 800-53| SP 800-37| NIST SP 800-171|FIPS| FISMA| FedRAMP| Risk Management Framework (RMF)| FIPS-199| PTA| PIA| SSP|CP|SAR|POA&M|ATO|ISA, MOU/A|IDS|IPS| Windows| eMASS.

Enterprise Mission Assurance Support Service| Linux| Microsoft Office||

**CAREER EXPERIENCE**

**Quash Consulting LLC,**

**Atlanta GA July 2019 - Present**

***Security Control Assessor***

* Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken.
* Develop/Review deliverables associated with a FedRAMP security authorization package including, but not limited to: System Security Plan, Information System Contingency Plan, Security Assessment Plan, Security Assessment Report.
* Perform cloud security assessments.
* Supports Security Control Assessments using NIST 800-53A Rev4 as guidance for current federal directives and policies.
* Performs System Security Categorizations using FIPS 199 and the NIST 800-60 Vol.11 Rev1 guidelines and templates to select provisional impact level assigned to the Confidentiality, Integrity and Availability (CIA) based on the information type.
* Analyzes and updates System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E).
* Develops and track Plan of Actions and Milestones (POA&Ms) to ensure remediation closure.
* Maintains and manages Security Authorization and Assessment packages that include System Security Plans (SSP), Contingency Plans (CP), POA&Ms, SAR, and other relevant security documentations for the system.
* Coordinating or conducting IT security audits.
* Perform security risk assessment and analysis of resources, controls, vulnerabilities, asset decommissioning, and information security threats to the organization’s objective.
* Review Nessus, WebInspect, and Nexpose scan reports for deficiencies and remediation of findings.
* Participates in the System Assessment and Authorization process by working with the key stakeholders to ensure complete and accurate ATO packages.
* Validated system requirements, security policies and procedures, contingency plans, incident response plans, personnel access control mechanism and identification.

**Metro IT Consulting LLC. Dallas, TX.**

**October 2017 - June 2019.**

**Information System Security Officer.**

* Identify, review, prioritize vulnerabilities and remediation efforts
* Experienced in performing Ongoing Security Authorizations aligned to NIST SP 800-53 and 800-137.
* Reported and maintained security architecture, policies, and compliance, identified and documented security vulnerabilities, system status; maintained records of incidents, hardware/software, etc
* Review for accuracy Security Control Assessment (SCA) documentation, including but not limited to the Security Assessment Report (SAR).

Conduct risk assessments, develop POA&Ms, facilitating and coordinating with information owners and custodians.

* Ensured POA&M mitigations and timelines were adhered to and documented any changes that occurred.
* Reviewed status of Information Systems for modifications and assessed the impact to current system accreditation.
* Selecting and implementing applicable security controls (technical, operational and management) using NIST SP 800-53 Rev 4/5 as a guide.
* Monitors the effectiveness of incident management and Service Request fulfillment and makes recommendations.
* Reviewing Privacy Impact Assessment (PIA) documents after a positive PTA is created and ensuring that PII findings are recorded in the System of Record Notice (SORN).
* Generating, reviewing, and updating System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements.
* Performing ongoing continuous monitoring (ISCM) using NIST 800-137 Rev 1 as a guide.
* Ensured appropriate changes and improvement actions are implemented as required.
* Maintained current knowledge of authenticator management for unclassified systems-NIST 171.
* Ensured compliance with protection requirements, control procedures, incident management reporting, remote access requirements, and system management for all systems under scope.

**M&T Bank, Louisville, KY**

***IT Compliance Analyst.***

**August 2015 – September 2017.**

Administered Assessment questionnaires to all vendors to determine the control effectiveness.

* Provided analysis and conducted virtual risk assessment to continuously determine the security posture at the vendor site.
* Interact with regulatory agencies, auditors, as well as other compliance entities to support investigations regarding system risks posture.
* Support internal controls and Information Technology risk assessment and mitigation procedures.
* Conducted Inherent risk assessments for all assigned third-party vendors/suppliers.
* Monitored and ensured third party relationship adhere to contracts, compliant with regulatory guidelines and tracked upcoming expirations.
* Conducted risk and security assessments and evaluated results with system owners and custodians.
* Assist in the creation and execution of the vendor management processes to optimize relationships with vendors and to deliver the best results aligned to business risk mitigation.
* Validated IT control implementations, performs risk-based audit, and performs walkthrough on controls.
* Participates as an integral part of the team, exhibiting ownership, follow-through, initiative, awareness, and effective communication with the IT team and management.
* Ensures that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments.
* Engages with appropriate teams to implement measures to mitigate or prevent identified privacy risks related to patients and technology.
* Participated in the development and implementation process for continuous monitoring of IT processes to ensure Analyzed data to aid in decision-making regarding the implementation of security countermeasures or risk mitigation; assisted in implementing countermeasures.
* Conducts assessment of the security and privacy controls implemented by an information system to determine the overall effectiveness of the controls and the vulnerability state of components, applications and databases residing within the system boundary.

|  |
| --- |
|  |
| **& QUALITIES:** |

**PERSONAL SKILLS Strong attention to details, Team builder and player, Good interpersonal communication skills, Results-oriented, Initiative and Creativity, Fast Learner, and Ability to adapt, Critical Thinking, integrity, multi-tasking, strong organizational skills, time management and organizational skills, Interpersonal skills, emotional, stability, Good in French.**