Jerry John Amegbedzi

[jjprivate89@gmail.com](mailto:jjprivate89@gmail.com)

Tel: 5139041704

**Experience Summary**

Amegbedzi Jerry John has over 5+ years progressive working experience in information assurance, risk management and security, including supporting government audits. He has extensive experience as an Information Security Analyst (ISO) and Information Assurance analyst. His skills and expertise are concentrated in the following areas:

|  |  |
| --- | --- |
| ●       IT Audit  ●       Cloud Security  ●       FedRAMP Compliance  ●       FISMA Compliance  ●       Audit Liaison | ●       Risk Management  ●       Vulnerability Assessment and Analysis  ●       Security Consulting  ●       Information Security Continuous Monitoring (ISCM) |

He possesses excellent analytical/strong initiative and qualifications required to excel and succeed including excellent customer relationship. He is always continuously improving himself and prepared to take on new challenges.

**Educational Background**

**Associate Degree BioScience Technology**

Cincinnati, Ohio

August 2014 to May 2017

**Experiences**

**CareerTech Consulting**

132 Washington Blvd Laurel MD 20707

July 2016 to Present

**Information Security Analyst**

* Managing and monitoring POAMs for the assigned systems using CSAM and paying great attention to the completion date of each POA&MS
* Verifying and validating that each POAM content is updated and is being assigned to the right engineer or POC to have them work on remediating the vulnerabilities for that POAM.
* Working with the ISSO to make sure all POAMs are closed before their due date and have all the attached evidences required.
* Assisting with continuous monitoring using NIST SP 800-137 as a guide to make sure the assigned system is secure and can effective perform normal operations without compromising it CIA requirements or compliance.
* Performs RMF assessment on several different environments at the Census Bureau using both scanning tools and manual assessment. Assessment included initiating meetings and interviews with various System Owners and Information System Security Officers (ISSO), providing guidance of evidence needed for security controls, and documenting findings of assessment in the SAR.
* Security Documentation: Develop and perform updates to System Security Plans (SSP), System Assessment Plan (SAP), Risk Assessments, Incident Response Plans, System Assessment Report (SAR) and draft Plans of Action and Milestones (POAMs).
* Performs evaluation of policies, procedures, security scan results, and system settings in order to address controls that were deemed insufficient during Security Assessment and Authorization (A&A), RMF and continuous monitoring
* Develop Solution to Security weaknesses: Developed solutions to security weaknesses documented in POAM using tools like Excel Spreadsheets, Cyber security Asset & management (CSAM) and Trusted Agency FISMA (TAF) and Corrective Action Plan (CAP). Assisted ISSOs create solutions to weaknesses based on system functionality and pre-existing architecture.
* Develop, review and amended Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST publications and industry best security practices.
* Develop policy and procedural controls relating to Management, Operational and Technical Controls for the Organization.
* Create System Security Plans, Risk Assessment, Security Assessment Report and Plan of Action & Milestones Report and Authorizing Official's Briefing Report.
* Apply appropriate information security control for Federal Information System based on relevant NIST SP.
* Conduct 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) to the designated approving Authorization Official (AO) to obtain the Authority to Operate (ATO).
* Amends IT security policies, procedures, standards, and guidelines according to department and federal requirements.

**CareerTech Consulting**

132 Washington Blvd Laurel MD 20707

May 2014 to July 2016

**Information Security Analyst**

* Performed and Operated Security Categorization using (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners selected stakeholders.
* Developed and conducted Security Test and Evaluation (ST&E) according to NIST SP 800-53A rev 3 and rev 4.
* Carried out continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements.
* Developed Security Assessment Plan (SAP) to initiate Security Assessment for low, moderate and high control information systems.
* Updated IT security policies, procedures, standards, and guidelines according to department and federal requirements.
* Conducted Security Control Assessment on General Support Systems (GSS), Major Applications and Systems to ensure that such Information Systems are operating within strong security posture.
* Responsible for developing a Security Control Assessor (SCA) strategy for the organization and assessing the management, operational, assurance, and technical security.
* Performed IT risk assessments, documented assessment results to ensure compliance with operating system, network, and application local and NIST security policies
* Reviewed and analyzed the findings that identify security issues on the system and compile results and finding into a final Security Assessment Report, along with assessments and recommendations for remediation.
* Prepared POA&M with identified weaknesses and suspense dates for each IS based on findings and recommendations from the SAR
* Ensured configuration management (CM) for security relevant AIS software, hardware, and firmware are properly documented.
* Collaborated with ISSO and POC's to prepare Authorization to Operate (ATO) packages and Reviewed Nessus vulnerability scan results. Prepared and submitted Security Assessment Plan (SAP) to CISO for approval.
* Developed and updated security plan (SSP), Security Assessment Report (SAR), Plan of action and milestone (POA&M). Monitored controls post authorization to ensure continuous compliance with the security requirements.
* Created reports detailing the identified vulnerabilities and the steps taken to remediate them (POAM)
* Participated in other team initiatives, to include development of comprehensive security awareness program; and audit response activities.
* Managed, developed, maintained and communicated company policies, standards (FISMA, NIST 800-18, 53, 53A, 53 Rev4, 30, 37, 60, 137) compliance, risk and business management, and configurations in accordance with industry standards and best practices.
* Conducted security control assessment to assess the adequacy of management, operational privacy, and technical security controls implemented.