**Barbara Adjei | CRISC | Security +**

Austin-Texas | Email: barbaraadjei27@gmail.com | Cell: 774-578-1711

Area of EXPERTISE

12 plus years of progressive experience in securing information systems in accordance with FISMA, NIST, ISO-27001, HIPAA and other regulatory guidelines and frameworks. Assessment & Authorization (ATO), Conducting System Security Control and Risk Assessment, Auditing Continuous Monitoring, System Security Plan (SSP), Contingency Planning, Incident Response, Disaster Recovery Plan, POA&M and Vulnerability Management, Policy Management, Project Management, Audit prep and support. VA Handbook/Directive 6500 and DoD 8500 series

TECHNNICAL SKILLS

NIST SP 800-53A | 800-37 | 800-34 | Agile | Scrum | Kanban | Risk Management Framework | FedRAMP| AWS | AZURE| Jira| Power BI | Splunk | QRadar |CyberArk | STIGs | Nessus| Qualys| PENTEST| ServiceNow| XACTA| RSA Archer| eMASS

PROFFESIONAL EXPERIENCE

**Cyber Security Analyst** April 2018 **–** Present

DCS Corps Littleton-MA

* Prepare, create, and review Authorization to Operate (ATO) packages and artifacts including the SSP, RA, CMP, ISCP, DRP, IRP and PIA for systems and facilities using NIST publications.
* Apply the knowledge of NIST SP 800-53A, 30, 37, etc. and AWS/Azure GovCloud requirements to select and assess Technical, Operational, Management/Administrative and Privacy controls for information systems
* Create findings (POA&Ms) and recommend mitigation strategies based on impact level and the likelihood of an exploit, as required by the Assessment and Authorization (A&A) SOP and NIST guidelines in order to obtain and maintain ATO.
* Work with Data Owner/ System Owner to categorize information systems (IS) to be able to select and apply the appropriate baseline controls based on NIST SP 800-60, SP 800-53A, FIPS 199/ 200.
* Monitor controls post authorizations to ensure continuous compliance with security requirements.
* Formulate security assessment reports and recommendations for mitigating vulnerabilities and exploits in the system.
* Review and update Information System Contingency Plan (ISCP) and Tabletop exercise After Action Report (AAR), Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)
* Perform Control Assessment by reviewing implementations statements and evidence to determine if they are implemented correctly, operating as normal and meeting desired objectives to make them compliant with the A&A requirements

**Information Security Analyst** May 2015 – March 2018

Perspecta Arlington-VA

* Worked with A&A team members and IT Managers to establish and define information security programs, resources, schedules, and tasks
* Applied the knowledge of NIST SP 800-53A, 30, 37, etc. and AWS cloud platform requirements to select and assess Technical, Operational, Management/Administrative and Privacy controls for information systems (IS)
* Documented test results, evidence, findings (POA&Ms) and recommended remediation to stakeholders based on system categorization, the likelihood and impact/criticality of an exploit, and in accordance with the Assessment and Authorization (A&A) SOP, VA Directives, Handbooks and NIST guidelines so that an ATO/ATC can be obtained and maintained.
* Worked with Cloud Services Providers (CSP) and 3PAO to review cloud solutions platforms and to manage vulnerabilities by regularly documenting remediation milestones till the vulnerabilities are completely mitigated and the POA&M is closed.
* Reviewed, analyzed and validated Vulnerability/technical scans like Nessus, Qualys, Database, and Penetration tests to identify security gaps/deficiencies and create findings to track their remediation.
* In compliance with Continuous Monitoring requirements, prepared, validated and maintained security documentation including System Security Plan (SSP), Contingency Plan (CP), Privacy Impact Assessment (PIA), Interconnection Security Agreements (ISA)/ Memorandums of Understanding (MOU)
* Prepared information systems for annual audits and external third-party security control assessments

**Information Assurance Analyst** March 2010 – Jul 2015

University of Massachusetts (UMASS) Memorial Hospital Worcester – MA

* Worked with the ISSO to establish and define security programs, resources, schedules, and risks
* Helped develop test plans and procedures and documented test results and exceptions.
* Conducted the IS Risk Assessment and documented the results in the RAR
* Monitored, reported and educated HIPAA Privacy compliance with facility employees
* Conducted walk-through, documented gaps, and developed remediation plans for each area of testing.
* Assisted in developing Audit Plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning, and Relationship with Vendors.
* Created and implemented all security documentations required for system Authorization and updated according to continuous monitoring requirement policies.
* Participated in security team meetings and rendered support to IT Security program, which included ensuring appropriate steps were taken to implement information security requirements for all IT systems.
* Coordinated with ISSOs and Privacy Officers to conduct security awareness training and education on expected rules of behavior for end-users.

EdUCATION & CERTIFICATIONS

Bachelor’s Degree in Information Security

Certified in Risk and Information Security (CRISC)

Security+

CAP (In progress)