Nana-Afriyie Osei-Poku

571-447-1911

NAG.MYAA@GMAIL.COM

|  |  |
| --- | --- |
| OBJECTIVES | Seeking an Information Security Analyst position in a growth-oriented organisation with focus on FISMA, System Security Monitoring, Risk Assessments, Audit engagements,Testing Information Security Controls and Developing Security Policies, Procedures and Guidelines. |
| SKILLS & ABILITIES | Ability to work effectively in teams, both as member and a leader. Excellent written and verbal communication skills. Detailed oriented. Strong analytical skills. Windows/ FISMA/ ST&E/ SA&A/ SSP/ SAP/ NIST SP 800 series Rev I. Vol. II (800-53A Rev. 4/ 800-37/ 800-60) FIBS 199/200 RMF / ISO frameworks/ Wireless Network, Microsoft Word/ Excel/ Project/ Access, PowerPoint,RiskVision / eMass |

EXPERIENCE   
 VIRGINIA HOSPITAL - Sr. INFORMATION SECURITY ANALYST – VIRGINIA (CONTRACT)

FEB 2017 – Till Date

* Conducts security assessment and IT Security documentation to determine the Security posture of the System in line with NIST Risk Management Framework RMF) and associated federal governance and policies.
* Reviews and develops IT Risk Cyber security programs, policies and procedures using industry frameworks (NIST AND HIPAA )
* Works with business units and third parties to evaluate the risk of vendor relationships.
* Performs risk assessments on third parties and translate IT risks into business risks.
* Documents identified risks and follow up on remediation activities through completion.
* Translates cyber risk into business risks and communicate this to business units
* Uses GRC tools to effectively manages user provisioning to guide against violation of SOD and Least Privileges.
* Provides ERP audit remediation to resolve segregation of duties violations (SOD) in end user roles.Password reset,Validity date extensions upon approvals for users.
* Resolves complex problems requiring detailed knowledge of ERP security configuration and development.
* Working on missing authorizations for the Business users.
* Identify, analyze and monitor IT control gaps and perform the documentation, implementation and testing of the entire IT security control compliance across VA.
* Gathers and reviews artifacts to develop Authorization packages (SSP, SAR and POA&MS) for information system to be granted ATO.
* Review and Assess privacy controls in compliance with Privacy Impact Assessment (PIA) and Privacy Threshold Analysis (PTA) using NIST 800-53.
* Conduct Information System Contingency Plan (ISCP) Table top exercise annually in line with Business Continuity Plan (BCP)

AT&T - SECURITY CONTROL ASSESSOR (CONTRACT)) FAIRFAX, VA AUG 2015 - FEB 2017

* Perform technical analysis and review of cyber security artifacts (SSP/ PIA/ PTA).
* Analyze and advise on the risk and remediation of security issues based on reports from vulnerability assessment.
* Assess general and application controls using the NIST SP 800 (i.e. 800-53 rev. 4) series guidance to produce Security Authorization documentation for the General Support Systems, Major Applications and Minor Applications and FISMA.
* Generate risk reports on all assessment findings based upon NIST 800-30. \* Create testing methodologies for security control assessment program.
* Identify risks associated with IT infrastructure, operations and applications.
* Identify and communicate IT audit findings to senior management and clients.
* Collaborate with Team Lead of other FISMA systems to ensure continued compliance with security control inheritance conditions.
* Provide best practices on how to efficiently and effectively audit the access controls and configuration management controls.

### **CAPITAL ONE BANK. it SECURITY ANALYST** (CONTRACT)- MARYLAND

### July 2013- AUG.2015

* Reviewed systems security plans to ensure that the plans in place meet the stated security requirements.
* Identified and selected baseline security control requirements for systems based on NIST SP 800-guidance.
* Initiated, coordinated and tracked the security weaknesses as they were discovered (POA&M).
* As a POA&M Coordinator, I assisted by collecting documentation and evidentiary artifacts from stakeholders needed to close out POA&M items.
* I provided POA&M quarterly reports to the ISSO on all the 8 Systems assigned to me.
* Prepared, validated, and maintained security documentation. (SSP/ RA/ CP/ PIA/ FIPS Categorization)
* Evaluated security and privacy controls to determine which are applicable to the system
* Continuous monitoring and collected data on the system performance.

BANK OF AMERICA ,– INFORMATION SECURITY COMPLAINT ANALYST ( CONTRACT ) NY, NY

OCT. 2011- JULY. 2013

* Performed technical analysis and review of cyber security artifacts (SSP/ PIA/ PTA).
* Analyze and advise on the risk and remediation of security issues based on reports from vulnerability assessment.
* Assess general and application controls using the NIST SP 800 (i.e. 800-53 rev. 4) series guidance to produce Security Authorization documentation for the General Support Systems, Major Applications and Minor Applications and FISMA.
* Generate risk reports on all assessment findings based upon NIST 800-30.
* Create testing methodologies for security control assessment program.
* Identify risks associated with IT infrastructure, operations and applications.
* Identify and communicate IT audit findings to senior management and clients.
* Collaborate with Team Lead of other FISMA systems to ensure continued compliance with security control inheritance conditions.
* Provided best practices on how to efficiently and effectively audit the access controls and configuration management controls.

EDUCATION

* Bachelors in Marketing- University OF Ghana LEGON 2004-2008
* Associate in Information system Management- IPMC, Ghana 2001-2003

CERTIFICATIONS

* Certified Ethical Hacker (CEH)
* CompTIA Security +

Reference will be provided upon Request

-