**Frank Britwum**
 Austin, Tx – 9732774355 – fbritwum06@gmail
 Authorized to Work in United States For Any Employer

**SUMMARY:**

Information Technology (IT) Assurance and Compliance Analyst with 12 years expertise in IT network and system security, regulatory compliance, risk and vulnerability assessment, test plan, continuous monitoring, authentication & access control, and IT policy compliance in large institutions. Experienced in federal Information Security Management Act (FISMA) guidelines, FIPS-199, NIST 800-53, NIST 800-30.

**Skills and Abilities:**

* Payment Card Industry Data Security Standard (PCI DSS)
* FEDRAMP
* Risk Management Framework (RMF)
* Security Assessment Reporting (SAR)
* System Security Plan.
* Continuous Monitoring (CM)
* FIPS 199/ FIPS 200
* Outlook 365
* Plan of Action and Milestone (POAM)
* HIPAA and HITRUST
* Microsoft Suit (Microsoft word, PowerPoint, excel, access)
* Windows 7,8,10

**SAIC** *October 2021 – Present*

**Senior Cybersecurity Engineer**

Responsibilities:

* Oversees Vulnerability analysis and assessment inspections, and audits and assessment/surveys.
* Analyzes and evaluates secured networks and recommends procedures and products to improve the overall security.
* Develop and implements policies and procedures to effectively implement a central scheme for systems management and control.
* Identifies critical operational problems and devises resolutions to include initiating innovative and unique methods in problem resolutions.
* Ensure systems/applications meet the necessary security regulatory compliance for their controls and cyber integrity.
* Designs and develops plans for implementing protective measures to prevent unauthorized access, disclosure, acquisition, manipulation, modification, or loss of information while it is being automatically processed or stored.
* Promptly reports system failures leading to the unauthorized disclosure of classified or otherwise sensitive information to appropriate security intelligence organization.
* Analyzes, identifies, recommends, and as appropriate, develops preliminary plans and concepts for modifications to system configurations and security plans.
* Monitors projects that will assign additional systems management support tasks to organizations to ensure the proposed architectures can be supported.
* Develop and generate vulnerability reports to senior management for awareness with IP360

**Halfaker & Associates LLC, Austin TX** *April 2016 – Oct 2021*

**Information Assurance Security Analyst**

Responsibilities:

* Independently develop Assessment & Authorization (A&A) packages (Risk Assessment, System Security Plan (SSP), Configuration Management Plan (CMP) and Contingency Plans, etc.)
* Kept track of the remediation efforts results, reviewed and uploaded documents to eMASS.
* Develop, review, and evaluate System Security Plans (SSP) and Information System Contingency Plans (ISCP) based on NIST Special Publications.
* Conduct all steps of the National Institute of Standards and Technology (NIST) Risk Management Framework.
* Ensure that system's security controls, policies and procedures are examined and validated.
* Conduct IT controls risk assessments that include reviewing organizational policies, standards, and procedures; interview appropriate personnel; and provide recommendations on adequacy, accuracy and compliance with regulatory standards using NIST SP 800-53A.
* Provide expert advice to developers, administrators, and others during system development life cycle.
* Reviewed Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU) for the team
* Assist in the Security Control Assessment (SCA) process using NIST 800-53/53A to improve security controls and enhance system security.
* Manage Plans of Action & Milestones (POA&M) and assist with remediation plans to resolve weakness in Risk vision
* Conduct and review vulnerability scans (Nessus, Web Inspect, IP360), make recommendations to senior leadership on how to resolve any vulnerabilities found.
* Act as the main POC expert for all security related matters for assigned systems.

**Wipro, Austin Tx**  *Jan 2015 - April 2016*

**Information Security Officer**

Responsibilities:

* Ensure that assigned information systems are operated, maintained, and disposed of in accordance with approved security policies and practices.
* Ensure that system security requirements are addressed during all phases of the IS lifecycle.
* Developing and maintaining the SSPs and all other system security documentation, reviewing and updating them at least annually for all assigned systems.
* Author or coordinate the development of other required system security plans: Configuration management (CM), Contingency Plan (CP), Continuity of Operations (COOP), Disaster Recovery Plan (DRP) and Incident Response Plan (IRP).
* Support risk assessment and evaluation activities throughout the system's lifecycle.
* Implement a strategy for continuous monitoring for assigned systems including Establishing system audit trails and ensuring their review, reporting all identified security findings, and initiating the periodic review of security controls.
* Requested or conduct required information system vulnerability scans in accordance to establish policy; Develop system POA&Ms in response to reported vulnerabilities.
* Ensure compliance with annual FISMA deliverables and reporting.
* Assessed and mitigated system security threats/risks throughout the program life cycle; determines/analyzes and decomposes security requirements at the level of detail that can be implemented and tested.
* Reviewed and monitored security designs in hardware, software, data, and procedures; performs system certification and accreditation planning and testing.
* Prepare C&A documentation such as SSP, CONOPS and ST&E reports.
* Responsible for designing, implementing, securing, and deploying a secure network architecture from the ground up for a startup company, supporting it throughout it increase in size over the course of many years.
* Personally, performed a variety of Cyber Intelligence assessments.
* Accountable for NIST standard risk management framework and architecture for the company.

**TATA Consultancy Services, Newark, NJ** *(March 2006- Dec 2014)*

**Information Security Analyst**

Responsibilities:

* Established and maintained an information assurance compliant framework (RMF) to ensure that information security policies, technologies and processes were aligned with the business regulations of the organization.
* Ensured that risk identification, mitigation controls and analysis were integrated into application life cycle and change management processes.
* Maintained computer security files to incorporate new software, correct errors, or change individual access statuses.
* Coordinated the implementation of computer system security plans with establishment personnel and outside vendors.
* Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy, and compliance with Federal requirements.
* Provided technical expertise on accessing HBSS configuration requirements based on STIG implementation guidelines.
* Designed and implemented a security assessment strategy to reduce risks via reporting and mitigating vulnerabilities, and assessing ports, protocol, and services based on DISA configuration standards.
* Coordinated vulnerability scanning and control assessment of all assets, operating systems, and databases utilizing Retina and Nessus, as well as applicable security manual checklists to validate compliance.
* Ensured the data recovery, data integrity, and database performance, availability, and maintenance were met through applying best practices and monitoring of policies, standards, and system processes relating to database management.
* Maintained computer security files to incorporate new software, correct errors, or change individual access statuses.
* Coordinated the implementation of computer system security plans with establishment personnel and outside vendors.
* Managed and facilitated the accountability and submission of all administrative duties and responsibilities of the team.

**EDUCATION:**

* Master of Cyber Security, UMUC, MD In Progress
* Montclair State University. Montclair, NJ Sep 2009 - June 2012

 BS, Administration (Marketing and Management)

* Bergen Community College. Paramus, NJ Sep 2006-May 2009

 AS, Accounting

**CERTIFICATION - ISACA**

* Certified Information System Auditor – (CISA)
* Certified Information Security Manager – (CISM)