***DIEUDONNE MBUNYA***

**Email:** [**dmbunya@gmail.com**](mailto:dmbunya@gmail.com)

**Contact:** 2402649085

**US Citizen**

**Profile**

An accomplished Cyber Security Analyst/Information Security Analyst/Assessor with 5 years of experience in directing, implementing, planning, and monitoring of security systems as well as managing authorization process on information systems. Experienced in RMF, NIST SP 800 Series, Risk management, Risk Assessment, Security Vulnerability Management with strict enforcement of regulatory compliance. Experience in Creating, developing, reviewing, And Analyzing security Documentation such as SSP, IR, SAR, SAP, CP/CPT, CM, SORN, FIPS PIA, and POA&M. Proficient in industry recognized SIEM (Security Information and Event Management) solutions, user intrusion-detection, vulnerability, and network security.

**Expertise**

* Information system authorization • Risk mitigation & management • Identity/ access management
* Risk management framework • Security training • Interviewing & collaboration
* Information system categorization • Organizational system
* Vulnerability Management • Regulatory compliance
* Creating SOPs.
* Risk Assessment
* Security Control Implementation
* Security controls monitoring

**Special skills**

Great Team Player, Excellent verbal, and written communication skills, Eager and willing to learn, Reliable individual. Strong monitoring skills function effectively with little or no supervision and meet date line. Strong Analytical skills and great leadership skills.

**Professional Experience**

**Security control Assessor, Washington Tech Solution. March 2021- present.**

* Support NIST Risk Management Framework (RMF) based Assessment and Authorization (A&A) activities.
* Monitor and prepare required actions and documents pertaining to the A&A of the system throughout its life circle to include security evaluation findings and residual risks.
* Conduct comprehensive reviews of security authorization documents to ensure the appropriate NIST SP 800 – 53 and 53A security guidelines were used during the assessments and the selections of security controls are relevant to the confidentiality, integrity, and availability of the systems.
* Ensure required security authorization activities are completed and the results are documented in the Information Assurance Compliance System tool.
* Review and process Interconnection Security Agreements (ISAs), Policy Waivers, Approval to Test (ATT), and Interim Approval to Operate (IATO) documents.
* Review Information system security plans and other A&A documents for all applications to determine if mandated procedures and tasks are followed.
* Ensure that assigned systems/applications meet the minimum A&A standards before a recommendation is made to the Authorization Officer.
* Attend Compliance Team meetings and provide reports in the approved format on the status of requested activities.
* Demonstrate experience in conducting security assessments.
* Conduct interviews assess operational needs, and reviewed artifacts to determine the Security posture of the System to develop a Security Assessment Report (SAR) and to meet accreditation requirements.
* Update and upload all pertinent information for all systems within the FISMA portfolio repository.
* Update relevant FISMA Compliance SOPs on a quarterly basis.
* Provide guidance and support for all assigned Security Authorization activities.
* Conduct Security Authorization entrance conferences.
* Develop a preliminary Security Assessment Report (SAR).
* Create the CSS Plan, including rules of engagement (ROE) for each major application, information system, or GSS undergoing authorization.
* Document the results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, analyze findings, and develop risk mitigation techniques to address weaknesses.
* Develop test procedures and/or document recommendations for test plan modifications that improve validation of control objectives.
* Obtain, review, and interpret organizational IT policies, standards, and procedures to identify control that would assist in mitigating risk.
* Review test results or interpret evidence for vulnerabilities, gaps, or control deficiencies and work with stakeholders to establish plans for sustainable resolution.
* Identify risks associated with control failures and support the identification of mitigating controls.
* Demonstrate experience providing threat analysis based on identified security vulnerabilities.
* Develops and documents security evaluation test plans and procedures
* Develop and provide all documentation necessary for performing a Security Control Assessment.
* Experience in Security Control Assessment Plan (SCAP), Scanning Authorization Requests, Access Requests, Security Assessment Report (SAR), and Security Technical Results, and other ad hoc system specific documentation as specified by the government.
* Ensures physical access request and authorization form and logs for all sites with controlled access to IT.
* Implement Identity Access Management (IAM) at user, data, and system levels for security

**Information security Analyst, CMnet Worldwide. Jan 2018 – Jan 2021.**

* Develops, review, and update Information Security System Policies, System Security Plan (SSP), and security baselines in accordance with FISMA, NIST SP 800-18, OMB, and industry security practices.
* Apply various NIST series in different projects, such as FIPS -199 & NIST SP 800-60 for information types categorization, NIST SP 800 – 53 & FIPS 200 for security control section, NIST SP 800 – 53A for security controls assessment, and NIST SP 800 – 18 for System Security plan development.
* Prepare ATO packages for system recertification and maintain all required documentations for ATO.
* Perform security control assessments and upload results to (CSAM) - Cyber Security Assessment and Management tool.
* Review and validate Plan of Actions & Milestones (POA&Ms) for each non-compliant control for each managed IT System prior to authorizing closure.
* Proper documentation to support the POA&M lifecycle shall be filed and updated as required, including well documented waivers and exceptions detailing the potential risk to the Authorizing Official.
* Perform in depth reviews of logs and other artifacts for each IT system
* Review and submit Change Request documentation – Security Impact Analysis
* Acted as a liaison for the program managers, system administrators, user representatives and developers to complete an entire A&A package in a timely, professional, and organized manner, which included the analysis and definition of security requirements.
* Document and Review security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies.
* Making sure that change management procedures are followed especially with patch management by making sure that the change request form are signed and validated before any change is carryout.
* Coordinate with engineers in Vulnerability scanning in making sure that they are perform per the agency policy and procedure and all vulnerability are being remediated.
* Thorough understand of and experience with the Federal Information Security Management Act (FISMA)
* Support independent security control Assessments for all assigned systems.
* Provide advice on proposed change request and work closely with auditors to identify key controls to be assessed.
* Manage POA&Ms and provide oversight of system vulnerability management
* Reviewing and updating system access authentication form and other documentation to ensure authorization are available complete and properly granted.
* Participate in all steps of the Security Authorization and Assessment process for FISMA systems.
* Deliver all required documentation using approved templates, forms, regulations, and methods.
* Ensure standard operating procedures (SOPs) are up to date.
* Verify all change request, and approval forms on file for any changes, including emergency changes.
* Ensure contingency plan is current and up to date
* Update controls in the Security Standard Document and implement cybersecurity practices such as clean desk policies, in collaboration with team members.
* Conduct security control assessments and compile the authorization package (System Security Plan, Security Assessment Report, and Plan of Action & Milestones).
* Prepare Assessment and Authorization package for company’s IT systems, ensuring regulatory compliance in assisting System Owners and Information System Security Officers (ISSO).
* Perform Information Systems categorization, and selection of controls based on impact levels of the system.
* Provide, track and report security requirements throughout the project life cycle of all projects that are within the authorization boundary of assigned systems
* Experience in preparing and reviewing authorization package (SSP, SAR, and POA&M) for companies to get an ATO or recertification.
* Strong writing skills to create documentation such as SOPs, internal process documents and input into cyber policies that support the continuous monitoring of accredited information systems.
* Working and documenting Risk Management Framework processing with end results achieving an Authorization to Operate (ATO).
* Performed vulnerability response and mitigation in compliance with the Information Assurance Vulnerability Management (IAVM) program.

**Cyber Security Analyst, Authors Path Academy . Jan 2016 - OCT 2017**

* Examine and review items uploaded into POA&M tracking tool in support of remediated/closed findings in compliance with FISMA.
* Prepared and reviewed Authorization to Operate (ATO) package such as SSP, SAR, and POA&M for major systems or applications.
* Conduct risk assessments, risk management and vulnerability management in support of the Information Assurance (IA) team.
* Ensure that vulnerability scans are perform on a recuring bases for every device running on the network per OMB.
* Ensure that prompt and time remediation of critical, high, and medium vulnerabilities as required by the organization policy are effectively remediated.
* Support and schedule remediation plan meeting with the engineers to effectively remediate findings.
* Experience in patch management in accordance with the system and organization change request procedures.
* Experience in Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), security events and logs from various security devices.
* Provided written recommendations for authorization concerning the impact levels for confidentiality, integrity, and availability for information on the system.
* Performed security and risk assessment of information systems and evaluated security documentation leveraging established testing and evaluation techniques and tools.
* Provided the organization with knowledge and guidance following NIST, information security and privacy.
* Vulnerability remediation activities, scanning and analysis and STIG/ Manual Checklist auditing
* Ability to work multiple projects concurrently within deadlines while ensuring that complex information is conveyed in a clear, accurate, and concise manner under normal and in crisis situations
* Skill in the use of various types of office automation to includes Microsoft Suite (PowerPoint, Word, Excel, Visio, Project, and Access)
* Superior verbal and written communication and customer service skills.
* Ability to work collaboratively and proactively with customers and program office members in a multi-vendor environment.

**Technical Skills**

**Domain:** Cyber security Analyst | SCA **|** IA**|** Compliance Analyst | ISSO.

**Database:** Oracle | OEM, RMAN | Database Microsoft SQL servers | SSMS

**Software:** Microsoft Office 365 | Word **|** Excel **|** Outlook | PowerPoint | Visio | Microsoft Windows Server 2016 | Nessus **|** Wireshark | Nmap | CSAM | basic Linux | Xacta.

**Education & Certifications**

**Bachelor’s Degree in Political Science 2009**

**Certifications:**

* CompTIA Security + Certified.
* Microsoft certified associate 70-462
* OCA (Oracle Certified Associate)
* AWS Certified solution associate
* CAP InProgress
* Certified safe 5 Scrum Master
* PSM 1