**UCHENNA NDOLO**

**Phone (240) 898-6759 |** [**uchenna.ndolo@yahoo.com**](mailto:uchenna.ndolo@yahoo.com)

**Clearance**

Public Trust

Secret - Eligible

**EDUCATION**

**Master’s in management of Information Systems • Information Assurance**

Bowie State University • Bowie MD • 2015

**Bachelor of Science in Finance • Finance**

University of Maryland University College • College Park MD • 2005

**CERTIFICATIONS**

Certified Ethical Hacker (CEH) 2017

Certified Information Security Manger (CISM) 2020

Certified Data Privacy Solutions Engineer (CDPSE) 2020

Certified Information Security Auditor (CISA) 2021

AWS Certified Developer -Associate- Sep 2018

CompTIA Security + Ce - 2015

Certification of Cloud Security Knowledge (CCSK) - Sept 2017

Cisco Certified Entry Networking Technician (CCENT) - 2015

Cisco Certified Network Associate (CCNA) - 2016

Information Systems Analyst Certification – 2015

**TECHNICAL EXPERTISE**

* Audit Readiness Assessment
* FISCAM, SAS 70/SSAE
* Microsoft Suit (Word, Excel, PowerPoint, Access, Project, Visio)
* SAP, Oracle Financials, PeopleSoft
* Financial Management/Internal Controls experience
* Health Insurance Portability Act (HIPAA), ISO 27001/2, FedRAMP, NIST Standards
* OMB Circulars A-123, A-127, A-134, A-136 and other OMB policies
* Federal Information Security Management Act (FISMA)
* Risk assessment, Audit engagement, testing information, and information technology controls
* Vulnerability Management tools: Nexus, Qualys, Veracode, etc.
* Governance, Risk Management, and Compliances (GRC) – RiskVision, eMASS
* IBM Rational Reporting
* SPLUNK, Active Directly.
* Cloud Computing AWS (EC2, RDS, Route53, Auto scaling, ELB, VPC, S3) 3PAO
* VMware Workstation, Virtual Box.
* Chef, Ansible, Jenkins, Dockers.
* Coverity, Blackduck and Netsparker
* FedRAMP assessment and assessment readiness/ 3PAO assessment verification

**PROFESSIONAL EXPERIENCE**

**Principal Cyber Engineer (SME)**

**Cognosante supporting VETERANS AFFAIRS Washington D.C, 03/2022- Present**

* Ensured information systems and application are compliant as mandated by appropriate Federal Department and Agency Regulations and Policies.
* Develop and deliver Business Continuity Plans, Contingency Plans and Disaster Recovery Plans that address and cover the IT systems supporting the technical needs of Decennial program and operations
* Support and lead the execution of privacy maturity assessments and risk assessments.
* Recommended areas for improvement and lessons learned
* Experience with advising Cloud Service Providers, preferably working for a 3PAO
* Design, plan and coordinate the implementation of disaster recovery test
* Apply risk management and Information Governance principles to our client’s data privacy and information protection environments.
* Assist in leveraging the existed back up processes to restore critical infrastructure
* Development of Disaster Recovery documentation
* Experience managing complex projects of a similar scope and complexity encompassing cloud computing, virtual networking, software application integration, big data, cyber security technologies, ecosystems, and architecture.
* Facilitate and conduct Disaster Recovery Tests
* Development of test plans and scenarios for Disaster Recovery Tests
* Understand global data privacy regulations (GDPR, HIPAA, CCPA, etc.).
* Experienced with Federal compliance initiatives, to include FedRAMP and FISMA
* Create Disaster Recovery test analysis report, which includes outcomes of the test
* Experience with NIST 800-37, NIST 800-53 and NIST 800-53a
* Guide clients through risk management and control implementation efforts.
* Collaborate with 3PAO’s to prepare application materials demonstrating that the organization meets both technical competence in security assessment of cloud systems and management requirements for organizations performing inspections
* Review and assess security assessment plan to include a comprehensive set of procedures for assessing the effectiveness of security controls employed in the cloud environment and enabling more consistent, comparable, and repeatable assessments of security controls customized for cloud applications
* Develop security assessment reports to include all the assessment results and assigned mitigation strategy for each risk; perform analysis on each finding to promote a better understanding of the risks to organizational operations; organizational assets, and individuals
* Develop NIST / FISMA / FedRAMP SA&A documentation for systems and networks undergoing certification and validate the quality of deliverables produced by the team
* Assess risks, identify mitigation requirements, and develop accreditation recommendations; be responsible for tracking SA&A requirements for assigned systems within the agency and validate that task are on schedule, and ensure the delivery of quality documentation
* Assist in the creation of SA&A packages with the responsibility for gathering information from system owners, applying data to the appropriate templates, and attending meetings in support of the effort
* Assist in responding to requests for information from OMB A-123, FISMA, GAO, and external auditors
* Support the implementation of data privacy compliance processes (e.g. DPIAs execution, Data
* Assessed organizational progress against existing security strategies, plans, or directives
* Conducted analysis of alternatives in response to customer requirement.
* Experienced assisting teams utilizing Agile Software Development methodologies to successfully integrate web services that have been certified and accredited following RMF and FedRAMP.
* Managed multiple Department of Veteran Affairs teams through the authorization and accreditation (A&A) process of GSS and MA.
* Wrote Security Assessment Report (SAR) and provided (POA&M) Plan of Action and Milestones with risk analysis. Attended weekly project security meetings.
* Developed policy, programs, and guidelines for implementation
* Evaluating system, network, or infrastructure security controls against requirements such as FISMA, FIPS, and NIST guidelines.
* Creating, reviewing, assessing, and monitoring POA&M, SSPs, Contingency Plans and other relevant security documentation for new systems. Implementing, Assessing, and evidencing Security Controls NIST 800-53 Rev4 for Cloud Environments (AWS, MAG-Azure).
* Expert knowledge of GRC Risk Vision.
* Responsible for A&A Scan requirements (Nessus, WASA, Database, and Fortify)
* Develop Security Assessment Plans (SAP) and Security Assessment Reports (SAR)
* Create corrective actions on how to remediate noted deficiencies
* Serving as SecureIT's primary POC and relationship manager for FedRAMP 3PAO clients
* Assisted FedRAMP teams to identify vulnerabilities and risks to CSP (Cloud service provider) accreditation.
* Modified and Identify FedRAMP Boundary components in customer deployments
* Coordinate with internal stakeholder engineering teams to demonstrate the implementation of security compliance control implementations for technical, management, and operational requirements
* Updated FedRAMP security control audit and evaluation
* Assisted Auditing security control to ensure compliance with cloud requirements and governance models

**Principal Cyber Engineer (SME)**

**GovernmentCIO supporting VETERANS AFFAIRS Washington D.C, 06/2019- 03/22**

* Ensured information systems and application are compliant as mandated by appropriate Federal Department and Agency Regulations and Policies.
* Develop and deliver Business Continuity Plans, Contingency Plans and Disaster Recovery Plans that address and cover the IT systems supporting the technical needs of Decennial program and operations
* Support and lead the execution of privacy maturity assessments and risk assessments.
* Recommended areas for improvement and lessons learned
* Experience with advising Cloud Service Providers, preferably working for a 3PAO
* Design, plan and coordinate the implementation of disaster recovery test
* Apply risk management and Information Governance principles to our client’s data privacy and information protection environments.
* Assist in leveraging the existed back up processes to restore critical infrastructure
* Development of Disaster Recovery documentation
* Experience managing complex projects of a similar scope and complexity encompassing cloud computing, virtual networking, software application integration, big data, cyber security technologies, ecosystems, and architecture.
* Facilitate and conduct Disaster Recovery Tests
* Development of test plans and scenarios for Disaster Recovery Tests
* Understand global data privacy regulations (GDPR, HIPAA, CCPA, etc.).
* Experienced with Federal compliance initiatives, to include FedRAMP and FISMA
* Create Disaster Recovery test analysis report, which includes outcomes of the test
* Experience with NIST 800-37, NIST 800-53 and NIST 800-53a
* Guide clients through risk management and control implementation efforts.
* Collaborate with 3PAO’s to prepare application materials demonstrating that the organization meets both technical competence in security assessment of cloud systems and management requirements for organizations performing inspections
* Review and assess security assessment plan to include a comprehensive set of procedures for assessing the effectiveness of security controls employed in the cloud environment and enabling more consistent, comparable, and repeatable assessments of security controls customized for cloud applications
* Develop security assessment reports to include all the assessment results and assigned mitigation strategy for each risk; perform analysis on each finding to promote a better understanding of the risks to organizational operations; organizational assets, and individuals
* Develop NIST / FISMA / FedRAMP SA&A documentation for systems and networks undergoing certification and validate the quality of deliverables produced by the team
* Assess risks, identify mitigation requirements, and develop accreditation recommendations; be responsible for tracking SA&A requirements for assigned systems within the agency and validate that task are on schedule, and ensure the delivery of quality documentation
* Assist in the creation of SA&A packages with the responsibility for gathering information from system owners, applying data to the appropriate templates, and attending meetings in support of the effort
* Assist in responding to requests for information from OMB A-123, FISMA, GAO, and external auditors
* Support the implementation of data privacy compliance processes (e.g. DPIAs execution, Data
* Assessed organizational progress against existing security strategies, plans, or directives
* Conducted analysis of alternatives in response to customer requirement.
* Experienced assisting teams utilizing Agile Software Development methodologies to successfully integrate web services that have been certified and accredited following RMF and FedRAMP.
* Managed multiple Department of Veteran Affairs teams through the authorization and accreditation (A&A) process of GSS and MA.
* Wrote Security Assessment Report (SAR) and provided (POA&M) Plan of Action and Milestones with risk analysis. Attended weekly project security meetings.
* Developed policy, programs, and guidelines for implementation
* Evaluating system, network, or infrastructure security controls against requirements such as FISMA, FIPS, and NIST guidelines.
* Creating, reviewing, assessing, and monitoring POA&M, SSPs, Contingency Plans and other relevant security documentation for new systems. Implementing, Assessing, and evidencing Security Controls NIST 800-53 Rev4 for Cloud Environments (AWS, MAG-Azure).
* Expert knowledge of GRC Risk Vision.
* Responsible for A&A Scan requirements (Nessus, WASA, Database, and Fortify)
* Develop Security Assessment Plans (SAP) and Security Assessment Reports (SAR)
* Create corrective actions on how to remediate noted deficiencies
* Serving as SecureIT's primary POC and relationship manager for FedRAMP 3PAO clients
* Assisted FedRAMP teams to identify vulnerabilities and risks to CSP (Cloud service provider) accreditation.
* Modified and Identify FedRAMP Boundary components in customer deployments
* Coordinate with internal stakeholder engineering teams to demonstrate the implementation of security compliance control implementations for technical, management, and operational requirements
* Updated FedRAMP security control audit and evaluation
* Assisted Auditing security control to ensure compliance with cloud requirements and governance models

**Principal Cyber Engineer (Lead)**

**Halfaker and Associates, LLC supporting VETERANS AFFAIRS Washington D.C, 03/2018- 06/2019**

* Ensured information systems and application are compliant as mandated by appropriate Federal Department and Agency Regulations and Policies.
* Develop and deliver Business Continuity Plans, Contingency Plans and Disaster Recovery Plans that address and cover the IT systems supporting the technical needs of Decennial program and operations
* Experienced with advising Cloud Service Providers, preferably working for a 3PAO
* Design, plan and coordinate the implementation of disaster recovery test
* Experienced managing complex projects of a similar scope and complexity encompassing cloud computing, virtual networking, software application integration, big data, cyber security technologies, ecosystems, and architecture.
* Experienced with Federal compliance initiatives, to include FedRAMP and FISMA
* Development of Disaster Recovery documentation
* Designed Cyber Security strategies that address the vision, mission, and goals of senior leaders and organizations
* Experience with NIST 800-37, NIST 800-53 and NIST 800-53a
* Analyzed existing security strategies, roadmaps, and implementation plans
* Assessed organizational progress against existing security strategies, plans, or directives
* Conducted analysis of alternatives in response to customer requirement.
* Experienced assisting teams utilizing Agile Software Development methodologies to successfully integrate web services that have been certified and accredited following RMF and FedRAMP.
* Managed multiple Department of Veteran Affairs teams through the authorization and accreditation (A&A) process of GSS and MA.
* Wrote Security Assessment Report (SAR) and provided (POA&M) Plan of Action and Milestones with risk analysis. Attended weekly project security meetings.
* Developed policy, programs, and guidelines for implementation
* Evaluating system, network, or infrastructure security controls against requirements such as FISMA, FIPS, and NIST guidelines. Creating, reviewing, assessing, and monitoring POA&M, SSPs, Contingency Plans and other relevant security documentation for new systems. Implementing, Assessing, and evidencing Security Controls NIST 800-53 Rev4 for Cloud Environments (AWS, MAG-Azure).
* Expert knowledge of GRC e. g Risk Vision, eMASS
* Responsible for A&A Scan requirements (Nessus, WASA, Database, and Fortify)
* Designing and configuring the AWS Secure Notification Service (SNS) and Secure Email Service (SES) architecture of the solution and working with a client.
* Ability to clearly document assessment results
* Managing IAM accounts (with MFA) and IAM policies to meet security audit & compliance requirements.

**Senior Information Security Analyst (Lead)**

**Accenture Federal Services supporting VETERANS AFFAIRS Washington D.C, 02/2016-** **03/2018**

* Serves as subject matter expert on both information security compliance topics as well as subject matter services on the tools, techniques, methods, and process that ensure information security across the department.
* Experienced in security policy development, metrics capture and analysis, security education, application vulnerability assessments, risk analysis and compliance testing, and project management.
* Conducts systems security evaluations, audits, and reviews; and develops Automated Information Systems (AIS) security contingency plans and disaster recovery procedures.
* Monitors and tracks-controlled access programs to ensure implementation and viability of appropriate systems security policies, as well as the acquisition of IT security tools.
* Reviewed and trained VA customers on NSOC scans reports on Web Application Security Assessment (WASA), Penetration Test reports, Secure Code Review, Secure Code Quality Review and Secure Code Design Review
* Ensure information security compliance efforts are part of business practice and information technology; develops and deploys resources to meet VA information Security requirements.
* Review project requirements, Implement, identifies deficiencies, and recommend solution in solving complex policy and compliance issues; Coordinated information security programs and privacy programs to meet current and future information management needs that comply with the vulnerability reporting standards and Government requirements.
* Support quarterly review efforts: Plan, analyze and evaluate the effectiveness of operating programs; Coordinate with program team members to gather and validate data; able to use qualitative and quantitative analytical skills to assess the effectiveness of the operations
* Ability to assess system security vulnerability and threat analyses, risk assessments and mitigation planning and implementation.
* Knowledge of information security rules and regulations related to information security and data confidentiality (e.g., HIPAA). Strongly engaged with security Engineers addressing network security principles for risk identification and analysis.
* Problem Solving - Proven record of accomplishment in meeting deadline and timelines by paying attention to detail Identifies problems; determines accuracy and relevance of information; uses sound judgment to generate and evaluate alternatives, and to make recommendations.

**Security Engineer**

**Valton Trans. Ellicott City, MD. 07/2015-02/2016**

* Positioned cyber security as the lifeline for all information security functions and developed inputs/outputs and processes for integrating with various groups like security strategy, security consulting, risk assessment, security detection and incidence response.
* Engineered, implemented, and monitored security measures for the protection of computer systems, networks, and information.
* Provided security architecture guidance that is built on principles of balancing security advice with business and IT needs. Performed gap analysis across the organization to identify unnecessary complexity in existing processes and procedures, work with service and application owners on mitigation strategies.
* Managed security incidents that cross multiple teams in the organization.
* Identified and defined system security requirements.
* Designed system security architecture and developed detailed security designs.
* Served as an information security advisor to key IT and business stakeholders, establishing trust relationships through active engagement and collaboration.
* Prepared and documented standard operating procedures and protocols
* Configured and troubleshoot security infrastructure devices.
* Established system wide information security requirements based on policy and regulatory requirements based on NIST 800-53 for client
* Wrote comprehensive reports including assessments -based findings, outcomes, and propositions for further system security enhancement
* Determined security requirements by evaluating business strategies and requirements; research information security standards; conduct system security and vulnerability assessments.
* Partner with Operations and Architecture team and stay abreast of business and industry technologies and trends.
* Developed technical solutions and new security tools to help mitigate security vulnerabilities and automate repeatable tasks.
* Performed gap analysis across the organization to identify unnecessary complexity in existing processes and procedures, work with service and application owners on mitigation strategies.

**Security Engineer (IT)**

***Unatek Inc.***  **Bethesda, MD. 09/2013-05/2015**

* Served as a member of Security team on Unatek high-profile client projects.
* Served as expert across security functional areas, including credential management, access provisioning, application security, infrastructure security, data security, security monitoring, and operational security across the organization. Partner with multiple projects and initiatives to apply security architecture requirements, develop solutions, integrate security into solution designs, assess risks, and develop architecture remediation.
* Served as lead or technical expert to define and maintain the architectural frameworks/patterns, processes, standards, and guidelines related to systems, business, or data architecture.
* Conducted analysis of new technologies to provide more efficient and cost-effective solutions. Research and recommend tools to help manage security analysis, process, and incident management.
* Developed methodology/framework for providing consistent and repeatable security architecture guidance to new projects by working alongside various IT teams and business customers and groups.
* Developed presentations for Division Chiefs that explain complex security topics in a very simple business-oriented language along with their business Monitored Security Information and Event Management (SIEM) for security incidents and performed incident response at Unatek.
* Supported clients at highest level in development and implementation of doctrine and policies.
* Developed project plans for all assigned security projects to ensure high-quality and timely delivery and to meet future requirements.
* Experienced in managing centralized patch and vulnerability management.
* Established and satisfied system-wide information security requirements based upon user analysis, policies, regulatory and resource demands.
* Developed project plans for security environment to meet future requirements.
* Implemented common controls into C&A package during contract procurement phase to ensure quick turnaround possible for Solution Provider’s C&A task.
* Established system wide information security requirements based on policy and regulatory requirements based on NIST 800-53 for client
* Developed and maintained System Security Plan a formal document to ensure it provided an overview of security requirements for information system and described security control in place to meet requirement of associated documentation
* Conducted periodic reviews (self-assessments). Assisted with information system Security audits, reviews, and report findings.
* Assisted in network troubleshooting by using standard methodology like determining the problem with the network, gather facts, define possibilities, develop action plan, execute plan, test result and document.
* Wrote Security Assessment Report (SAR) and provided (POA&M) Plan of Action and Milestones with risk analysis. Attended weekly project security meetings.
* Used network management commands like ping for verification on communication between networks

**Security Analyst**

***Iweanoges Law*. Washington, DC. 09/2009-07/2013**

* Performed testing of IT general and application controls, identify deficiencies in the design and operating effectiveness of controls and provide recommendations.
* Evaluated the design and effectiveness of technology controls throughout the business cycle.
* Evaluated the adequacy and effectiveness of the client’s internal controls using a risk-based methodology developed from professional auditing standards and frameworks, such as COBIT and FISCAM.
* Prepare audit scope, reported findings, and presented recommendations for improving data integrity and internal controls.
* Develop audit work program and detailed understanding audit activities, including IT risks and controls, internal control strengths and weaknesses.
* Assisted in the drafting of audit reports to summarize audit findings
* Complete work papers in compliance with department requirements

**Tax Accountant**

**Namcro Tax service. Riverdale, MD. *01/2005-07/2009***

* Assisted in yearly preparation and submission of virtually error-free personal and business tax returns. Verified compliance with all applicable federal and state tax code regulations.
* Educated clients on tax preparation, forecasting and liability reductions strategies.
* Assembled trouble-shooting teams to resolve tax issues due to unique client circumstances.
* Corresponded with Internal Revenue Service for compliance opinions and guidance to protect clients’ best interests.
* Trained service staff to enhance customer services and increase profits through suggestive selling and innovative.
* Worked as part of a team that determined the integrity of the security system for a company.
* Tested policies put forward by a company to determine whether there are risks associated with them.
* Reviewed and interviewed members of the staff to learn about any security risks or other complications within the company