|  |
| --- |
|  |
| **PROFILE** |
| Information Technology and Health Services professional with CISM, AWS, Security +, and ITIL certifications and ten-plus years of experience. Specializes in Governance, Risk Management, and Compliance (GRC) and in developing and securing cloud solutions to satisfy business needs. Has a track record of collaborating effectively with multiple stakeholders and advancing cross-functional teams to capture exact requirements, deliver innovative solutions, and keep IT risks at levels acceptable and consistent with organizations’ risk appetite. |
| **CERTIFICATIONS & TRAININGS** |
| * Certified Information Systems Manager (CISM)
* Security +
* Agile Methodology
 | * AWS Certified Solutions Architect – Associate
* ITIL Foundation
* HIPAA/HITECH
 |
| **PROFESSIONAL EXPERIENCE** |
| **Program Manager III | 01/2022 – 07/2022** | **Wimmer Solutions - Seattle, WA** |
| Contracted to Microsoft to provide oversight, tracking, and reporting for high-priority and time-sensitive initiatives for vertically integrated security processes maintained by the Edge & Platform, Devices, and Gaming Security (EDGS) division of Microsoft’s business.  |
| * Established and maintained a collaboration and communication framework for monitoring and reporting progress on action items, deliverables, and requisites for OKRs and KPIs.
* Managed the Rhythm of Business (ROB) to minimize workflow disruptions, improve time utilization, and ensure proper integration of new processes, ideas, technologies, and projects to the rhythm and agile method.
* Supported the development and continuous updates for Security Solution Plans (SSP) and manages the documents, meetings, and dedicated channels for improving and promoting the plans.
* Delivered automated solutions with Power Automate, Planner, Lists, and SharePoint to improve collaboration, requirements gathering, and the quality of project deliverables.
* Produced data points and visuals that show the current state, rate of utilization, and effectiveness of service initiatives with Excel and Power BI.
* Manages projects’ sprints and tracks team’s progress on Azure DevOps.
* Set clear timelines and workback schedules that advance desired goals and aided in removing progress blockers.
 |
| **Senior Risk & Compliance Officer | 02/2015 - 01/2022** | **CSAAC - Montgomery Village, MD** |
| Guided the development and implementation of AWS cloud solutions for the organization’s business needs and coordinated the Security Compliance, Risk Assessment, Systems Authorization, Continuous Monitoring, Audit Support, and Security Controls Selection and Assessment efforts for cloud information systems.* Advanced the development and adoption of standards, procedures, and guidelines that align IT risk management with the organization’s goals, strategies, and vision.
* Ensured information systems and personnel comply with HIPAA/HITECH rules, HITRUST framework, and NIST guidelines 800-37, 800-53, and 800-30, in support of Authority to Operate (ATO) objectives.
* Maintains the Security Authorization Package that includes the System Security Plans (SSP), Contingency Plans, Security Assessment Reports (SAR), POAMs, and other relevant security artifacts.
* Gathered periodic requirements from internal and external stakeholders and worked with developers and architects to build cloud-centric solutions to exploit opportunities, improve efficiency, mitigate risks, and comply with adopted standards.
* Collaborated with specialist teams to design and develop technically sound and HIPAA/HITRUST compliant, cloud-native Electronic Health Record (EHR) System to improve collaboration with health care providers and enhance health information storage, access, sharing, and security.
* Assessed AWS systems’ configurations for built-in failovers, storage backups, proper lifecycle management, fault tolerance, version controls, optimized throughput, authorized connections, and up-to-date security requirements.
* Provided subject matter expertise in risk management and compliance for multiple cloud projects and helped new and existing systems meet the requirements to pass Assessment and Authorization (A&A) tests.
* Monitored and analyzed cloud systems' performances, vulnerabilities, security controls, and compliance measures with AWS services, including CloudWatch, CloudTrail, GuardDuty, Inspector, and Config, and took appropriate measures to reduce the likelihood and impacts of identified risks.
* Examined and tested Contingency Plans (incidence response, disaster recovery, and business continuity plans), evaluated their completeness, and developed appropriate remedial actions to correct errors and improve processes.
* Prevented unauthorized access to data, resources, and environments by enforcing granular access control with AWS Identity and Access Management (IAM) tools, including service control policies, IAM Access Analyzer, and MFA.
* Designed an AWS Simple Workflow Service (SWF) application that simplified work coordination across departments and helped reduce citations for non-compliance with industry regulations and standards by 60% over two years.
* Configured highly available, cost-effective, and fault-tolerant compute and networking systems by leveraging autoscaling, elastic load balancing, and multi-AZ in systems’ design
 |
| **Security Analyst | 01/2012 - 02/2015** | **Strategic Intelligence Technologies, Laurel, MD** |
| Promoted, executed, and enforced cybersecurity policies and Information Assurance (IA) standards for the US Marshals Service (USMS) in accordance with NIST’s RMF. Supported key personnel’s continuous efforts to maintain a certified and accredited system that satisfies operational requirements and the desired security posture of the client’s information systems. * Wrote custom Security Test and Evaluation (ST&E) plans and reports to support the certification and accreditation efforts at the USMS and prepare systems for FISCAM-guided audits.
* Implemented technical test case strategies and procedures for various operating systems, database environments, and applications, per` NIST, FISMA, FIPS, and USMS ’s security policies and requirements.
* Conducted requirements assessments with Nessus, CIS tools, and documentation reviews to determine the effectiveness of implemented security controls based on NIST SP 800-37, 800-53, and 800-53A.
* Monitored and assessed systems, applications, and programs to validate compliance with defined benchmarks and investigated instances and suspected instances of unauthorized access and compromise of the system’s defenses.
* Completed and updated System Security Plans, Risk Assessment Reports, Certification and Accreditation packages, and other IA documents that include Business Impact Assessments (BIA), Security Assessment Reports (SAR), and Privacy Impact Assessments (PIA).
* Prepared reports with findings and recommendations to correct identified vulnerabilities, manage security updates, and deploy security patches.
* Developed timely POAMs and remediation plans for the vulnerabilities identified during risk assessments, routine audits, and inspections.
* Assessed Contingency and Configuration Management plans, reported findings and provided inputs and recommendations to improve risk mitigation strategies.
 |
| **EDUCATION** |
| * 2015 | M.Sc. Health Systems Management
* 2004 | B.A. Mass Communications
 | University of Baltimore, Baltimore MD Babcock University, Nigeria |
| **EXPERTISE & CAPABILITIES** |
| * IT Governance, Compliance & Risk Management
* Health Systems Management
* Cloud Solutions
 | * IT Service Management
* Security Research, Monitoring, and Analysis
* Data Privacy, Analytics, and Visualization
 |
| **OTHER SKILLS** |
| * **Microsoft Suite**: Word, Excel, PowerPoint, SharePoint, OneDrive, Power BI, Power Automate, Teams
* **Google Workspaces**: Drive, Docs, Sheets, Slides, Vault, Calendar
 |