**Michael A. Adjetey**

Greater Dallas/Fort Worth, Texas Area | 214.998.7049 | [madjetey97@yahoo.com](mailto:madjetey97@yahoo.com)

linkedin.com/in/michael-adjetey-8248a5132

**Cybersecurity/ Security Architect**

**A Specialist in** **information systems security strategy, governance, risk mitigation, & compliance**

Accomplished professional with over thirteen years of progressive responsibility guiding talented teams to implement responsive security initiatives and solutions to enhance enterprise-level services. Passionate about working in collaboration with the infrastructure, applications and data teams to identify, design and manage the completion of security risk detection, mitigation programs, audits and compliance.

**CORE PROFICIENCIES**

Enterprise-Level Security Systems & Services | Vulnerability Assessments & Audits | Cybersecurity Governance |

Security Operations Management |Regulatory Compliance | Security Compliance | ServiceNow IRM |

Critical and Analytical Thinking | Strategic Thinking | Communication and Coordination | Network Security |

Creative | Innovative | Problem-Solving | Detail Oriented | Technical Writing | Positive Thinker | Logical | Intuitive |

Solution-Oriented and Innovative | Problem Resolution | Team Leadership and Mentoring

**Technical Skills**

|  |  |
| --- | --- |
| ***Advanced Microsoft Office Suite***  ***IS Management Frameworks***  ***Risk Analysis Methodologies***  ***Regulatory Compliance***  ***Security Awareness***  ***Governance Risk & Compliance (GRC) /*** ***Integrated Risk Management (IRM)*** | Word, Excel, PowerPoint, Publisher  NIST 800 series, CSF, ISO 31000, 270xx, ITIL, COBIT, FFIEC  NIST, OCTAVE, Service Now, Salesforce, Process Unity, On Trust, Archer  GRC, GLBA, SOX, SOC, HIPAA, Hi-Tech, PCI-DSS, CSA STAR, ISO Proof point, Knowbe4, Infosec IQ  Policy & Compliance Management, Risk Management, Vendor Risk |
| ***Cloud Models*** | IaaS, SaaS, and PaaS (Public, Private, Hybrid) |
| ***Security*** | IDS/IPS, HIPS, NIPS, ATD/TIE, Anti-Virus, firewalls, 3rd Party Risk Assessment |
| ***Vulnerability Tools*** | Rapid7, Nexpose’, Nessus, Qualys |
| ***Environments*** | Windows 10, Server 2012, 2016, AS400, Unix, Linux, Active Directory |

**Career Highlights**

* **Over 11 years of experience in Insurance, HealthCare, Banking, Government, and IT based Industries as a Senior Security Architect.**
* **Excellent problem solving, communication, and interpersonal skills; self-motivated with good work ethics.**
* **Ability and willingness to learn new programs fast.**
* **Good understanding of BA Methodologies relative to the Software Development Life Cycle (SDLC).**
* **Extensive experience in gathering and documenting business and functional requirements and communicating effectively with upper management.**
* **Good facilitation skills in conducting walkthroughs, surveys, interviews, brainstorming and Joint Application Development.**
* **Good experience in working closely with Quality Analysts for reviewing business requirements, functional requirements, documenting test scenarios and writing test cases.**
* **Experience in using use-cases, creating test scenarios and test scripts using requirement documents.**

**PROFESSIONAL EXPERIENCE**

**EC3 Federal Services**

Accenture Federal June 2023 to September 2024

**Lead Cybersecurity/ Application Specialist**

* Using Agile principles and practices to design, develop, test and deploy scalable and secure SaaS solution for Third Party Risk Management.
* Engage with team members, product owners and other stakeholders in an Agile refinement sessions to understand and prioritize customization requirement.
* Implement changes iteratively, seeking feedback and iterating based on user input to ensure alignment with evolving needs.
* Design, develop, implement, and maintain the identity and access management procedures to ensure proper user account provisioning. Collaborate with other information technology personnel to ensure solution designs have appropriate information security controls
* Develop and maintain metrics to track adoption rates and regularly assess and enhance security controls, conducting assessments and evaluations to ensure effectiveness and compliance with established standards.
* Lead the implementation and delivery of Third-Party Compliance initiatives.
* Design and develop process workflows and reports using Third Party vendor platform ProcessUnity.
* Develop a detailed quality assurance plan and execute quality assurance steps to deliver a quality product.
* Develop, deploy, and refine processes that identify pain points to deliver operational and technical improvements
* Communicate with technical and non-technical audiences at various levels to influence and manage implementation of the solution.
* GRC/IRM Consultant who has experience implementing ServiceNow
* Collaborate with key stakeholders to develop new, and update existing policies, procedures, and standards, required to support the project outcomes. Define and implement an ongoing security risk assessment program, which will define, identify, and classify critical information assets, assess threats and vulnerabilities regarding those assets and implement remediation plans where appropriate in certain security functions. Provide guidance of security risk assessments of third party relationships and associated corrective actions
* Assist in the information security incident response process and provide guidance to senior management related to incident escalation and resolution. Assist in the preventive monitoring of potential information security threats, investigation of alleged information security breaches and, if necessary, drive appropriate response to the breach
* Collaborate with delivery teams to design, develop, and implement secure solutions

**W.R. Berkley** June 2022 to August 2023

**Information Security Architect**

Coordinates the implementation of system security plans with agency personnel and outside vendors.

* Define and implement an ongoing security risk assessment program, which will define, identify, and classify critical information assets, assess threats and vulnerabilities regarding those assets and implement remediation plans where appropriate in certain security functions. Provide guidance of security risk assessments of third party relationships and associated corrective actions
* Act as the lead architect, making critical decisions around ServiceNow IRM modules and integrations.
* Develop and maintain metrics to track adoption rates and regularly assess and enhance security controls, conducting assessments and evaluations to ensure effectiveness and compliance with established standards.
* Provides Technology risk expertise while working with Technology teams, and other risk partners (e.g., Independent Risk Management, Compliance, Audit).
* Develop User Acceptance Test plans
* Develop Unit Test Plans
* Assist in develop End-to-End Quality Assurance plan
* Conduct regression test after each deployment
* As an admin Salesforce, I was responsible for managing and customizing Salesforce to meet your organization’s needs. This includes user management, data management, reporting.
* Lead the design and implementation of Risk Management (IRM) solutions on the ServiceNow platform.
* Lead Security Reviews for Production Deployment - Oversee security reviews and authorizations to ensure systems meet security controls, risk management requirements, and compliance with regulatory standards.
* Lead Governance Frameworks: Leverage expertise in governance, compliance, and strategic policy-making to enhance the organization's security frameworks, including certification and accreditation processes.
* Provide regular updates to senior leadership on system security, risk posture, and release status, ensuring informed decision-making.
* Continuously assess and refine security authorization and release management processes to ensure scalability, efficiency, and responsiveness to evolving security threats.
* Proactively identify gaps in security controls, processes, and documentation. Develop and implement solutions to improve the efficiency and effectiveness of the security authorization process.
* Lead the implementation and delivery of Third-Party Compliance initiatives.
* Configure and write code using native language provided by the vendor platform. This is a critical requirement.
* Design and develop process workflows and reports using Third Party vendor MetricStream.
* Develop a detailed quality assurance plan and execute quality assurance steps to deliver a quality product.
* Develop, deploy, and refine processes that identify pain points to deliver operational and technical improvements
* Communicate with technical and non-technical audiences at various levels to influence and manage implementation of the solution.

**Silicon Valley Bank**  Feb 2021 to May. 2022

**Manager InfoSec Team**

.

* Provide support by assessing systems suitability, obtaining and documenting user’s requirements documents, and assisting in data analysis.
* Supports execution of the Technology risk management program to meet business and regulatory expectations. Leads in the design and development of technology controls for specific technology risk management program components. Review current controls.
* Leads specific team while assisting with meeting or exceeding department goals.
* Sets clear performance expectations and holds direct report accountable.
* Ensures that goals are being translated to the team as they relate to tracking and productivity.
* Creates and nurtures an environment that emphasizes motivation, empowerment, teamwork, continuous improvement and a passion for providing service.
* Acts proactively when dealing with employee concerns.
* Extends professionalism and courtesy to employees at all times.
* Communicates/updates all goals and results with employees.
* Meets semiannually with staff on a one-to-one basis.
* Establishes and maintains open, collaborative relationships with employees.
* Solicits employee feedback
* Experience implementing ServiceNow Admin
* Assess and document internal controls over financial reporting to ensure accuracy and compliance.
* Conduct tests of controls to evaluate their effectiveness and identify any weaknesses or gaps.
* Risk Assessment: Perform risk assessments to determine areas that require more robust controls or monitoring.
* Work closely with finance, IT, and operational teams to ensure all processes align with requirements.
* Manages matters and issues to completion while meeting deadlines.
* Leads or influences technology risk initiatives and business as usual activities. Identifies risk, assesses impact and makes recommendations on resolution. Reports and escalates risk and program compliance as appropriate.
* Develop process, procedures for programs
* Collaborate with stakeholders while operating under the oversight of Auditor in Charge or Senior Audit Manager
* Monitor vendors for potential security incidents and act as the primary point of contact for incident investigations involving vendors Create process documentation, including workflows, process maps, & controls

**Consulting Firm: Nesco Resources**

**End Client: L3Harris, Link.** Jan 2020 to Jan. 2021

**Lead | Information Application Security Engineer**

* Implement security and anti-tamper controls into training and simulation solutions
* Interact with customers to define Cyber security and anti-tamper requirements, trades, solutions, costs, implementation, system impacts, and effectiveness
* Assist programs and monitor program execution throughout product development lifecycle to ensure cyber and anti-tamper objectives are met. Review and assess the security posture of cloud services, prepare findings and recommendations for certification.
* Proactively identify gaps in security controls, processes, and documentation. Develop and implement solutions to improve the efficiency and effectiveness of the security authorization process.
* Lead the implementation and delivery of Third-Party Compliance initiatives.
* Review third-party audits and reports (SOC, ISO, PCI DSS, HITRUST, etc.)
* Work with cloud vendors to communicate deficiencies in assessment responses
* Assist in streamlining/improving TX-RAMP workflows, processes, notifications, guidance, and communications.
* Develop and deliver security training programs for developers, IT staff, and other stakeholders.
* Create training materials, documentation, and presentations to educate teams on vulnerability management best practices.
* Develop and maintain metrics to track adoption rates and regularly assess and enhance security controls, conducting assessments and evaluations to ensure effectiveness and compliance with established standards.
* Review and implement security policies to ensure compliance with regulatory requirements and organizational standards.
* Implement industry security frameworks (especially FFIEC) and translate these into tailored, prescriptive control environments to guide security program investments in people, process, and technology
* Assess and develop security program policies, procedures, standards, and guidelines which are aligned to industry best practice and account for applicable compliance/regulatory requirements
* Provides Technology risk expertise while working with Technology teams, and other risk partners (e.g., Independent Risk Management, Compliance, Audit).
* Identify and evaluate risks associated with IT processes and systems, and recommend mitigation strategies.
* Develop, implement, and maintain IT security policies, procedures, and standards.
* Ensure compliance with industry regulations and standards (e.g., GDPR, HIPAA, SOX) by conducting regular audits and assessments.
* Manage user access rights and permissions to ensure that only authorized personnel have access to sensitive information.
* Coordinate the response to IT security incidents, including investigations and reporting.
* Conduct training sessions for staff on IT security best practices and policies.
* Maintain detailed documentation of IT controls, procedures, and incidents for audit and compliance purposes.
* Monitor IT systems for unusual activity and vulnerabilities, utilizing various security tools
* Collaborate with business unit employees and ERM team members on a variety of projects with a focus on risk quantification, developing reports and presentations.
* Work with leadership and help develop Risk Policy, procedures, and training materials.
* Analyze and report on an organization’s infrastructure through tools such as Splunk. Design processes and systems, based on the business model and its integration with technology.
* Manage and prioritize multiple assessments Lead the development and implementation of the corporate-wide IT risk management program to ensure information security risks are identified and continuously monitored.
* Systems Administrator Experience Experience with formulating and crafting vulnerability management policies and standards
* Risk management involving ongoing monitoring and evaluation of processes
* Routine auditing for compliance to vulnerability management policies and standards
* Understanding of vulnerability management.

**Consulting Firm: Odyssey Consulting**

**End Client: The Exchange (Dept. of Justice – Retail)** Sept2017 to Jan 2020

**Cybersecurity Engineer | Architect**

* Provided strategy and direction. Design and enforce pragmatic and consistent Information Security policies. Ensured traceability of security compliance including policy adherence, testing and remediation.
* Assist with identification and remediation of PCIF Plan of Action & Milestones (PO&MS).
* Identify existing and/or potential organizational security weaknesses as a result of the assessments, including personnel controls, training, incident and emergency response, logical security controls, physical security controls, operational security and integrity of software applications and data for customer engagements.
* Develop and deliver reports and presentations required for communicating findings of the security control assessments.
* Conduct vulnerability assessments on networks, servers, websites and databases, as
* Oversees and manages relationships for assigned systems that may be contractor-owned and contractor-operated, ensuring vendors comply with agency security and privacy requirements.
* Supports the development and maintenance of all security documentation such as the System Security Plan, Privacy Impact Assessment, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, annual FISMA assessment, and incident reports.
* Salesforce admin support responsible for managing and customizing Salesforce to meet your organization’s needs. This includes user management, data management, reporting
* Assist in the execution of the client's information security program, including meeting PCI compliance requirements.
* Responsible for security risk management operations including facilitating the identification, reporting, management and remediation of cybersecurity risks companywide. Practice planning, time management, negotiation, and delegation skills.
* Provide IT Security, risk management leadership and guidance. Plan and Execute Special Security Projects as Needed. Lead Security Remediation Activities.
* Work directly with delivery teams to provide guidance and ensure solutions adhere to security policy and best practices.

**Samsung Electronics America (SEA)** March2014 to June 2017

**Project Manager/ InfoSec Team Lead**

* Define and implement an ongoing security risk assessment program, which will define, identify, and classify critical information assets, assess threats and vulnerabilities regarding those assets and implement remediation plans where appropriate in certain security functions. Provide guidance of security risk assessments of third-party relationships and associated corrective actions
* Conducted research, impact & stakeholder analysis, scope determination, and determined the level of effort to complete requirement elicitation under Agile Scrum methodology.
* Develop User Acceptance Test plans
* Develop Unit Test Plans
* Defined the breakdown of tasks, resource loading, issue tracking, and resolution management.
* Collaborated with cross-functional teams to clearly document business needs as requirements in user stories to clearly actionable outcomes and expectations.
* Elicited, analyzed and translated business needs into consumable requirements/stories for the technical teams and ensuring that requirement statements are complete, consistent, concise, comprehensible, traceable, feasible, unambiguous, and verifiable, and that they conform to standards.
* Provided analytical support for multiple, complex cross-functional initiatives simultaneously, established work plans and timelines; coordinated with internal and external resources.
* Led Joint Application Design sessions with business and outside stakeholders.
* Engaged Business in an interactive design session to build IT Application architecture using UI/UX design.
* Led the development of business processes mapping designs using ARIS with the Business
* Collaborated with Project Manager to develop, prepare, and analyze reports for management review.
* Review and implement security policies to ensure compliance with regulatory requirements and organizational standards.
* Implement industry security frameworks (especially FFIEC) and translate these into tailored, prescriptive control environments to guide security program investments in people, process, and technology
* Assess and develop security program policies, procedures, standards, and guidelines which are aligned to industry best practice and account for applicable compliance/regulatory requirements
* Develop security program strategies and recommendations along with affiliated roadmaps and project plans – this may involve facilitating and delivering security program workshops and discovery sessions to assist clients with defining an overarching strategy for their security program
* Develop deliverables and presentations for client leadership which could include requirements documentation, gap analysis, program maturity models, short/long term program roadmaps and security tool rationalization outputs.

**Cybervision Technology** Feb 2012 to Dec 2014

**Security Systems (ISSO)**

* Lead a SOC 2 Audit at M3 USA. With a checklist provided by my team. Scope, Internal Risk Assessment review, Gap analysis, Implementation appropriate controls etc.
* Ability to conduct an analysis of the NIST SP 800-53 rev. 5 controls and identify controls that can be automated
* Ensures all systems are operated, maintained and disposed of IAW documented security policies and procedures including but not limited to Assessment & Authorization (A&A).
* Oversees and manages relationships for assigned systems that may be contractor-owned and contractor-operated, ensuring vendors comply with agency security and privacy requirements.
* Supports the development and maintenance of all security documentation such as the System Security Plan, Privacy Impact Assessment, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, annual FISMA assessment, and incident reports.
* Conduct Self-Annual Assessment (NIST SP 800-53A).
* Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems.
* Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard (PCI-DSS).
* Broad knowledge of relevant standards (e.g. COSO, COBIT, NIST, FFIEC, ISO, etc.).
* Strong interpersonal skills with ability to communicate effectively (fact based and credible), build relationships, challenge, negotiate and use professional judgment when working with key stakeholder across broad functions and geographic regions
* **THREAT & VULNERABILITY MANAGEMENT ANALYST**
* Collaborate with CCB Cyber Security, Global Technology Infrastructure, Corporate Cyber teams, and Line of Business Information Risk Management teams for issue resolution and mitigation
* Support innovation and enhancement efforts within the CCB Cyber Security function
* Analyze penetration test results and engage with technology partners and business units in order to resolve identified vulnerabilities within SLAs
* Understand approaches for addressing vulnerabilities including system patching, deployment of specialized controls, code or infrastructure changes, changes in development processes, cloud and mobile devices
* Identify and resolve any false positive findings in assessment results
* Documents all issues and assists in their resolution
* Delivers security training and education to technical staff within findings and acts as an internal security consultant to advise or influence business or technical partners

**EDUCATION & CREDENTIALS**

**Bachelor of Business Administration, Management Information Systems**

|  |  |
| --- | --- |
| CISA, Security Professional, ISACA |  |
| ITIL V3 Foundation  Security +  Juniper Networks FW/VPN Boot camp |  |
|  |  |

**Awards**

Best Security employee at Samsung 2017

InfoSec Award at Silicon Valley Bank