**John Davies**

(484) 781-2114 • daviesjpm@gmail.com



Over five years of experience in system security monitoring, auditing and evaluation, C&A and Risk Assessment of GSS (General Support Systems) and MA (Major Applications). Looking to obtain an information technology compliance position in an organization in critical need to secure its operations, processes and assets.

Excellent problem-solving abilities | Excellent communication skills | IT security best practices | Regulatory & Compliance |Team Player| Documentation | Data Analysis |Risk mitigation and Management |Automation| SaFe Agile | Fedramp | Windows | NIST



***S.I.A. Partners Inc. – Horsham, PA***

*INFORMATION SYSTEM SECURITY OFFICER (ISSO) Jan 2022-present*

* + Assisted Clients to write Memos when the POA&M findings are not remediated by the Schedule Completion Date.
  + Conducting IT controls assessments that include reviewing organizational polices, standards, procedures and guidelines.
  + Provided mitigation strategies and recommendations to key stakeholders to enhance their security posture.
  + Implemented company policies, technical procedures and standards for preserving the integrity and security of data, reports and access.
  + Assisted in the development of an Information Security Continuous Monitoring Strategy to help companies in maintaining an ongoing awareness of information security (Ensure effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions; FISMA Reports, Standard Operating Procedures (SOP) in accordance with Federal, Agency and Organizational policy, to include FISMA, NIST, OMB, and FIPS guidelines.
  + Consistently met deadlines and requirements for all production work orders.
  + Interface all levels of management and partner with other groups such as Engineering, Operations, Customer care and IT teams

***Liberty IT Solutions - Herndon, VA***

*Risk Management Framework Analyst Sep 2020- Jan 2022*

* Ensure that security processes and procedures are in line with **DoD/VA** information security policies and standards.
* Work with System Engineers, Senior Information Systems Security Engineers (Senior ISSOs) and Information Systems Owners to develop and maintain the System Security Plans (SSPs) and associated documentation
* Develop the configuration management plan and engineering documentation for security policy and implementation activities.
* Conduct impact level categorizations for Confidentiality, Integrity, and Availability of the information on a system
* Conduct implementation statement reviews and create implementation statements
* Utilize the RMF tool (EMASS) to upload artifacts and select controls.
* Develop, coordinate, and test Contingency Plans, Disaster Recovery Plans, and Incident Response Plans.
* Review system security documentation to accommodate changes to policy or technology.
* Assess changes in systems, environment, and operational needs that could affect accreditation.
* Develop, maintain and manage Security Authorization and Assessment packages that include System Security Plans (SSP), Contingency Plans (CP), and other relevant security documentation for existing and new systems.
* Review proposed change requests related to system design/configuration and performing a security impact analysis (SIA) to provide approval or denial recommendations.
* Implement and manage Security Controls in accordance with the current revision of NIST 800-53
* Conduct system certification tests, inspections, and reviews that include verification that the features and assurances required for each protection level are in place, and prepare Security Assessment Reports
* Review and analyze vulnerability scans to support Assessment & Authorization (A&A) activities
* Provide continuous monitoring to enforce client security policy and procedures and create processes that provide increased visibility to system owners on impacts on the security posture of systems
* Develop, maintain, and facilitate the appropriate closure of POA&Ms and any related remediation activities.

***Doylestown Health - Doylestown, PA*** *June 2018 to Oct 2020*

*Cyber Security Analyst*

* Knowledge on HIPAA Compliance Issues and Enforcement Rules. Audited/Implemented safeguards and controls, for the protection of client (PII) and data. Maintained/Updated tools to ensure protection of PHI in accordance with notification requirements.
* Prepares Security Assessment and Authorization (SA&A) packages to ensure that management, operational and technical security controls, conform and adhere to NIST SP 800-53 standards.
* Serves as the subject matter expert in giving client advice on the necessary steps to take to mitigate risk.
* Conducts kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-53
* Conducts security control assessments to assess the adequacy of management, operational, privacy, and technical security controls implemented.
* Develops Security Assessment Reports (SAR), Plan of Action and Milestones (POA&M) detailing the results of the assessment. Develops system security plans to provide an overview of federal information system security requirements, and describe controls set in place to meet those requirements.
* Creates and update the following artifacts; Security Assessment and Authorization (SA&A); Security Test and Evaluations (ST&Es), Risk assessments (RAs), Privacy Threshold Assessment (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs).
* Conducts IT controls risk assessments including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with industry standards.
* Develops risk assessment reports that identifies threats and vulnerabilities.
* 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.
* Review, interpret, analyze and reconcile security policies and standards to IT frameworks like ISO 27000.

***Prospect Holdings (Contractor) – East Orange, NJ***  *November 2016 to June 2018*

*Cyber Security Analyst*

* Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60.
* Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M).
* Assist System Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53.
* 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.
* Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages.
* Conducted I.T 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.



**EDUCATION and CERTIFICATION**

**CompTIA Security+ Certified**

**Certified Information Security Manger**

**Bachelor in Business Administration**

CUNY Lehman College New York, NY

**Associate in Computer Science**

CUNY Borough of Manhattan Comm. College New York NY

