IT Security Analyst IT Security Analyst IT Security Analyst Canal Winchester, OH An accomplished Information Technology Specialist with over 5 years' experience in Cyber Security, IT Audits, Risk Management, and Security Control Assessment. Adept at assessing controls, solving problems creatively and making strategic decisions in a fast-paced manner and communicate well at all levels. An Information Security Analyst with vast experience in Managing and Protecting Enterprise Information Systems, Network Systems and Operational processes through Information Assurance Controls, Compliance Verifications, Risk Assessment, Vulnerability Assessment in accordance with NIST, FISMA, OMB and industry best Security practices Work Experience IT Security Analyst Nesco Resource, LLC - Columbus, OH January 2017 to February 2019 Conducted IT risk assessment and recommended countermeasures to mitigate adverse impact. Developed test plans and testing procedures; documented test results and exceptions. Conducted walkthroughs, created test plans, and documented test results; developed remediation plans for incident response. Supported information security governance, risk and compliance activities aligned with the NIST. Risk Management Framework (RMF) Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60. Developed the audit plan and performed the General Computer Controls testing of Information Security, Business Continuity Planning. Identified gaps, developed remediation plans, and trained and advised IT managers on the SOX/FISMA compliance activities and controls. Helped business unit elaborate and identify internal control process. Manually reviewed logs and provided documentation guidelines to process owners and management. Developed, maintained and communicated a consolidation risk management activities and deliverables calendar. I do evaluate cyber crisis processes, tools and proficiency in responding to cyberattacks from both a strategic and technical response perspective by using tabletop exercise for medium and sometimes low systems. Developed the audit plan and performed the General Computer Controls testing of Information Security. Conduct continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements. Also did vulnerability scanning with SIEM Tools Splunk, a little on Nessus. Cyber System Analyst State Auto Insurance - Columbus, OH December 2015 to January 2017 Conducted kick-off meetings to collect systems information and

categorize systems based on NIST SP 800-60 Developed security control baseline and tested plan used to assess and implement security controls. Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Risk Assessments Report (RAR) Privacy Threshold Analysis (PTA), Privacy Impact Analysis. (PIA), Contingency Plan, Security Test and Evaluations (ST&Es), E-Authentication, Plan of Action and Milestones (POAMs). Designed and Conducted walkthroughs, formulated test plans, tested results and developed remediation plans for each area of the testing. Conducted FISMA complaint security control assessments to ascertain the adequacy of management, operational, technical privacy controls. Examined events logs for irregularities. Identified irregularities are then reported as incidents. The incident response is then initiated to mitigate these irregularities. Involved in security incident management in order to mitigate or resolve events that have the potential to impact the confidentiality, availability, or integrity of information technology resources. Created and maintained security metrics in order to help senior management to make decisions. Provide support to internal and external audit teams in gathering evidence to validate controls. Interviewed ISSOs, System Owners System Engineers and reviewed existing system documentations in order to make an objective assessment if the system complied with established standards. I build and maintain cybersecurity playbook to identify and list all possible actions that could occur in response to the initiating condition. IT Security Analyst Diligent Consulting - Columbus, OH November 2014 to December 2015 Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB, NIST SP 800-18 and industry best security practices. Develop and update System Security Plan (SSP), Privacy Impact Analysis (PIA), System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M). Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60. Develop policy and procedural controls relating to Management, Operational and Technical Controls for the organization. Conduct Security Control Assessment on General Support Systems (GSS), Major Applications and Systems to ensure that such Information Systems are operating within strong security posture. Update IT security policies, procedures, standards, and guidelines according to

department and federal requirements. Review and update some of the system categorization using FIPS 199. Conduct continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements. Put together Authorization Packages (SSP, POA&M and SAR) for Information systems to the Authorization Officer. Threat detection with SIEM tools Splunk Develop Security Assessment Plan (SAP) to initiate Security Assessment for low, moderate and high control information systems. Security Control Assessor ManTech International Corporation - Dayton, OH January 2014 to November 2014 Scheduled and led kick off meetings with system owners to help identify assessment scope, system boundary, the information system's category and attain any artifacts needed in conducting the assessment. Maintained information security governance, risk and compliance of activities within NIST Ensured that established internal control procedures were compliant by examining reports, records, documentation and operating practices. Performed continuous monitoring on asset vulnerabilities, prioritized vulnerability list and addressed critical weaknesses in the systems. Conducted FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations; conducted out-briefings. Work with a team of Information System Owners, Developers and System Engineers to select and Implement tailored security controls in safeguarding system information. Develop POA&M (Plan of Action & Milestones) to remediate actions resulting from security control assessments, monitor and track remediation progress using Risk Vision GRC. Perform assessment of ISs, based upon the Risk Management Framework (RMF) or the JAFAN 6/3 process. Education NATIONAL INSTITUTE OF INFORMATION TECHNOLOGY - ACCRA, GH 2009 Additional Information SKILLS Communication Ability to Work Under Pressure Decision Making Self-motivation. Conflict Resolution Adaptability Risk Management Framework. Create, Modify, and Update Security Information Event Management (SIEM) Tools. Splunk GRC NIST, ISO2700x, HIPAA Cyber and Technical Threat Analyses Similar Tools Demisto, Symantec, Palo Alto

Name: Anthony Drake

Email: john49@example.net

Phone: +1-801-917-8289x960