Baltimore , Lead Sr. Assessor Baltimore , Lead Sr. Assessor Baltimore , Lead Sr. Assessor - Arch Systems Inc Upper Marlboro, MD To utilize and enhance my skills, secure full time employment. I am a Subject Matter Expert on the FISMA Risk Management Framework and NIST (800-53), ISO 27000, FISMA,FIPS 199, DIACAP, HIPAA, SOX and PCI DSS standards.. Work Experience Baltimore , Lead Sr. Assessor Arch Systems Inc July 2018 to Present Lead a team of 12 security control assessors doing assessments on CMS systems using the New Adaptive Capability testing method. Create Security Assessment Report (SAR) based on assessment results Reported to C Level executives' assessment synopsis and system risk. Developed common practices for developing standards for assessing based on the SCA and Capability method. Mapped PCI DSS and HIPAA compliance to NIST standards. Managed 4 assessments a week from kickoff meeting to final out brief. Advised technical staff on best practices for Arch Systems security posture. Developed and managed scanning process for technical team on assessments. Oversee Arch systems Security Awareness program. Developed security baselines for hardware and networking devices for Arch systems. Wrote corporate security policies (Telework, Access control, SDLC, Configuration management policies). Documentation reviews for Contingency plans, System security Plans and Risk Assessments for inaccuracies. Performed Risk assessments for CMS using the Capability assessing method. Performed 3rd party vendor risk assessments for Arch systems. Lead Assessor Blue Canopy/HHS - Rockville, MD September 2017 to July 2018 Contract ended Lead and support Third Party security control assessments based on NIST SP 800-53 Rev 4. Create documentation for control assessment such as Kickoff slides, SCA Plan, SCA Report and debrief documentation. Analyze results from vulnerability scanning tools such as Nesses, Webinspect and App detective. Interface with clients related to the overall security control assessment program and all security control assessment activities. Which includes but not limited to: ? Review Contigency Plans ? Review SDLC Policies ? Review Incident response plans ? Review Configuration Management Plans ? Review System Security Plans ? Review Security Impact Analysis ? Review Risk Assessments Review Evidence for control failure Review evidence for assessment and help create POAMs for assessments. Develop, implement, review and evaluate System Security Plans, Interconnection Security Agreements, Privacy Impact Analysis's , Privacy Threshold Analysis's SRTM's, Risk Assessments, Plan of Actions and Milestones (POAMs), Security Assessment Reports, and Contingency Plans to satisfy Assessment and Authorization (A&A) requirements in accordance with DoDI 8510.01 and NIST Risk Management Framework, and other government guidelines as required.   Analyze application, database and operating system, scans and map findings to controls for POAM creation.   Develop, implement and/or review policies and procedures as required by various NIST security controls as well as PCI compliance.   Conduct periodic reviews to ensure compliance with established policies and procedures ensuring all software, hardware and firmware changes recorded as required by established configuration management procedures.   Participate in the configuration management process by reviewing changes for security impacts to the systems and participating in the Change Review Board process.   Ensure systems are operated, maintained and disposed of in accordance with applicable governing policies and procedures.   Perform IS security briefings, report all security incidents to the ISSM, and investigate, document and report, as well as provide protective and corrective measures in response to such incidents.   Coordinate and participate in special projects concerning information security, including testing and implementation of security software enhancements.   Develop, facilitate, and present information security awareness and security training on various customer and corporate security policies.   Serve as the company Information System Security Officer for a number of government accredited systems.   Maintain a broad knowledge of technology, equipment and/or systems to include the configuration, maintenance of firewalls, various operating systems, and phone switches   Support and maintain the physical security standards for Sensitive Compartmented Information. Seidcon/USPTO Information System Analyst USPTO 2016 to August 2017   Review evidence for assessment and help create POAMs for assessments.   Develop, implement, review and evaluate System Security Plans, Interconnection Security Agreements, Privacy Impact Analysis's , Privacy Threshold Analysis's SRTM's, Risk Assessments, Plan of Actions and Milestones (POAMs), Security Assessment Reports, and Contingency Plans to satisfy Assessment and Authorization (A&A) requirements in accordance with

DoDI 8510.01 and NIST Risk Management Framework, and other government guidelines as required. Analyze application, database and operating system, scans and map findings to controls for POAM creation. Develop, implement and/or review policies and procedures as required by various security controls. Conduct periodic reviews to ensure compliance with established policies and procedures ensuring all software, hardware and firmware changes recorded as required by established configuration management procedures. Participate in the configuration management process by reviewing changes for security impacts to the systems and participating in the Change Review Board process. Sr. Information Assurance Analyst- Risk Management Arlington, VA February 2015 to August 2016 Reason for leaving: Position relocated Providing best practices and guidance on Third Party Controls Assessments. Mapping PCI compliance to a Hybrid Security Information Guidelines. Executing and evaluating Third Party controls assessments and evidence for controls gaps and assisting with the documentation of any required remediation plans Assisting with the design and implementation of effective continuous testing and reporting processes and tools for infrastructure controls Assisting with the continuous improvement of the IT - Third Party Oversight Controls Assessment process and documentation Assist vendors with scanning applications, databases and applications as needed, Assist vendors with patch management solutions where needed. Assist vendors with vulnerability management and remediation techniques as needed, Collaborate closely with Third Party Oversight to provide Information Security Risk Assessment support for security assessments of E*TRADE vendors Complete security risk assessments, determine mitigating controls, document identified security risks, and track the corrective action through Management Action Plans (MAPs) as required. Execution of Third Party Control Reviews including onsite reviews, WebEx and phone. Collaborate closely with Business owners to define action plans to track gaps/needs across the technology organization specific to Third Party controls. Participate in meetings with IT managers and staff to understand E*TRADE's Third Party controls including management of processes and tools. Understand areas to improve risk management posture and recommend corrective actions and new standards. Refine process documentation to align with Regulatory requirements and best practices as noted through organizations such as BITS, ISO, and COBIT Provide reporting and metrics that ensure the quality of the program's services are meeting business objectives Foresees organizational impacts and understands the procedures associated with introducing new technologies and processes Coordinate \ participate as Subject Matter Expert for assigned onsite review activities for ensuring Information Security controls are being properly met and documented. Coordinate \ participate as Subject Matter Expert for assigned onsite review activities for ensuring Information Security controls are being properly met and documented. IT Security Engineer FDA - College Park, MD 2013 to February 2015 Reason for leaving: Contract ended Develop and maintain information security documentation for Customers major applications in accordance with Federal Departmental and Agency guidelines, including but not limited to: System Security Plans, Security Risk Assessments, Plans of Action and Milestones (POAMs), System Categorization Worksheets, Privacy Impact Assessments, Contingency Plans, Business Continuity Plans, Memoranda of Understanding (MOU), Interconnection Security Agreements (ISA), Rules of Behavior, and eAuthentication Risk Assessments. Review and provide guidance on software development life cycle (SDLC) documents for the Customer programs and provide development support for this documentation as needed. Review server and workstation scans and provide direction for remediation. Cloud Computing Security Implement Security Awareness Training program. Provide security oversight to old and new projects. Provide assistance as needed to support annual audits of Customer systems and programs, including drafting responses to audit reports. Update Incident Response forms, Track PII incidents, update the incident database, review and revise draft Personally Identifiable Information (PII) Breach Notification Packages. Information System Security Engineer KSJ- 5203 Leesburg Pike - Falls Church, VA October 2012 to September 2013 Reason for leaving: Contract ended. Served as ISSE on ATO efforts, Risk assessments, Annual Review's and Self assessments. Run scan on DOD web applications using Webinspect. Run scan on databases using Appdetective. Run cans on DOD GOTS/COTS systems using HP Fortify. Run manual checks against government systems using DOD Application Security and Development checklist (8500). Run Retina scans on IT systems and respond to IAVA compliance issues. Served as advisor on CIRT team. Serve as an advisor on Information Assurance matters. Run scans on IT systems and report vulnerabilities. Ensure DHSS Information Assurance program requirements are properly implemented. Assist in the development of accreditation packages Continuously review all System Security Accreditation Plans and complete re-accreditation actions as required. Ensure that proposed system changes are reviewed, and that changes, enhancements, or modifications implemented do not adversely impact system security features. Change Control advisor. that all Information System users of assigned systems are monitored to verify compliance with established security policies and procedures. Investigate and report actual or suspected Information System Security incidents, events or violations. Review system user practices and procedures for possible vulnerabilities that may pose a threat to system security. Ensure compliance with proper media/equipment control, handling, labeling, and disposition procedures. WMATA Contractor NFF - Washington, DC October 2011 to October 2012 Reason for leaving: Contract Ended Scan systems for vulnerabilities and recommend remediations. Manage firewall configuration. Provide technical expertise to clients, management and staff. Work with System owners to remediate POAM's. Administrator for content filtering software. Manage DLP solution. Create internet usage reports. Assist with HIPAA and PCI audits to make sure PHI and PII is secure in transit and at rest.. Counsel employees on privacy and Security. Investigated Change Control request. Created SOP's. Revised outdated IT policies. Assist with Security Awareness Training. Monitor IDS traffic for security threats. Discovers and mitigates security vulnerabilities. Respond immediately to any type of threats to determine the risk and set priority for resolution. Works with various IT office and departments to provide security expertise and guidance. Enforce patch management of production & test servers on WMATA network. Assist with enforcement of compliance for Security Awareness Training. Support incident response program. Respond to day to day operational issues. Participates in other program related activities. Security Engineer/Privacy and Compliance Officer MedAssurant - Bowie, MD August 2010 to October 2011 Reason for leaving: Long hours, no work life balance. Identifying and/or providing technical analysis of security requirements necessary for the protection of all information processed, transmitted and at rest. Scan systems and recommend remediation's for vulnerabilities. Manage DLP Solution. Perform physical security vulnerability and risk assessments as it relates to physical HIPAA compliance ie protecting PHI and PII for 6 locations across the United States. Perform Network scans and recommend remediation to network team. Consult with network team for server hardening for HIPAA compliance and protecting PHI and PII in transit and at rest. Responsible for server and workstation baseline configurations in accordance with HIPAA compliance regulations as it pertains to protecting PHI and PII.. Responsible securing PHI in accordance with HIPAA and PCI regulations. Assist in PHI audits as it relates to compliance with HIPAA and PCI regulations. Monitor network changes using Tripwire network monitoring tool. Create reports for internet usage for management staff using WebSense content filtering. Created incident response plan and incident response team. Functioning as a liaison between the corporation and security system and application vendors. Designing, maintaining, delivering and enhancing security awareness and training throughout the business. Providing advice and assistance on the interpretation of security requirements. Conduct/lead corporate investigations for missing or stolen assets. Monitor IDS traffic. Create technical and physical incident reports for HIPAA compliance violations. Information Assurance Analyst Department of Transportation - Washington, DC November 2008 to August 2010 Reason for leaving: Contract ended. Did C & A's on Government IT Systems. Part of a 3 person team that implemented FRA's continuous monitoring program. That process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information sharing decisions involving the enterprise. Work with system owners to remediate POAM's. Security control assessments. testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system or enterprise Change control board. Committee that makes decisions regarding whether or not proposed changes to the network should be implemented. Security Awareness Trainer. Making sure users understand that there is the potential for some people or organizations to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. Interact with DOT personnel on a daily basis in developing security policies, supporting its Certification and Accreditation (C&A) efforts using NIST publications 800-53, 800-37 , responding to computer security incidents, and troubleshooting and resolving any IA related problems. Track and report compliance status and associated deviation documentation per reporting guidelines as needed. Ensure information assurance requirements are implemented, documented, and verified on servers. Create and Maintain diagram of all network devices for enterprise using Microsoft Visio. Track and remediate network incidents. Network/System/ Security Engineer AFBA - Alexandria, VA January 2005 to November 2008 Reason for leaving: Career Advancement. Made sure all systems met baseline standards to meet NIST 800-53A requirements for FISMA. Provide day-to-day security maintenance and on-going security auditing. Served as Asset Manager for all network devices. Create and maintain documentation as it relates to network configuration and security policies. Explore , test and implement new technologies. Manage DLP solution. Active Directory admin. Served as backup helpdesk manager. Tier III Help Desk Tech Develop and implement security policies and procedures Install, configure, and manage IPS system (Active Scout). Create Ghost Images for servers and desktops. Manage various small to mid IT projects. Build and manage production servers. Create and manage FTP servers and accounts (Globalscape). Scan network for vulnerabilities and create reports (Tenable Nessus SC3) Manage patch software and deployment of necessary patches (Patchlink). Build and manage ticketing system BMC Remedy, Service Desk Express Create incident reports using BMC Remedy Service Desk Express (Crystal Reports.). Manage Change Control module of BMC Service desk Express. Developed and managed content filter proxy server (Smartfilter) Generated internet usage reports (Smart Reporter). Managed Malware Software (pest patrol). Ensure all machines on network had current virus signatures (Symantec 10.02). AD, Dell Open Server Mgmt, rebuild servers Dell Service

Provider- Qualxserv- Tewksberry, MA January 2003 to January 2005 January 2003 - January 2005 Reason for leaving: Get into the IT security field. Troubleshoot and replace Dell hardware (Laptops, Printers, Desktops and Server)components. Test hardware for functionality. Load software (Win2K, AD, Dell Open Server Mgmt, rebuild servers) to replace hardware. Configure hardware for Dell Servers. Provide Customer Service Training to entry level technicians. Manage 10 technicians during installation and troubleshooting of Dell systems. Load and configure applications. Perform manual data migration. Install peripherals (PDA's, scanners, printers, etc.) Provide Tier I help desk support Greater Southeast Community Hospital South Capital St , SE - Washington, DC February 2002 to January 2003 Washington DC- (Help DeskTechnician) February 2002 - January 2003 Provide Tier I help desk support. Create and Manage user accounts in Active Directory. Install, configure and troubleshoot pc's and network printers. Replace PC components as needed. Monitor inventory of PC's and components. Help desk Technician DC Government March 1998 to February 2002 Provide Tier I help desk support. Configure, troubleshoot and install PC's. Provide help desk support telephonically to clients. Provide inventory control for all PC's.

Name: Elizabeth Gibson

Email: martha25@example.org

Phone: 641.790.6109x2086