Consultant Consultant Information Security Professional CNY Please note: For security reasons, I will not perform an online, video recorded interview. Authorized to work in the US for any employer Work Experience Consultant Security and Complance April 2018 to November 2018 Helped bring company into PCI compliance for annual filing in June. This involved performing a PCI DSS 3.2 gap assessment; completing the SAQ D, setting up ASV scanning, performing scans and remediation; CIS benchmark scans for secure system configurations; firewall configuration and rules review; OWASP top 10 web application scans; risk assessment, wifi testing; physical controls review of the data center; access review; some security awareness training; writing the monthly security newsletter; setting up user activity monitoring and reporting; building data flow diagrams; and responding to malware incidents. ASsisted another company with achieving ISO 27001 certification. Much of the work was project oriented in helping the company close gaps found during an independent 3rd party audit. Gaps that would need to be closed to achieve certification. Consultant Security and Compliance January 2018 to March 2018 ScaleSec Private Consulting Firm. Joined ScaleSec consulting team on a project with one of their clients to complete preparatory work for SOC 2 Type 2 2018 assessment with Trusted Services Criteria, COSO and using ISO27001 framework. This involved controls analysis and documenting all of the client's processes and procedures, and control activities and providing evidence to the assessor. After SOC 2 assessment, began working on ISO 27001 certification. I performed a gap analysis of SOC 2 controls against the 27001 Annex A controls. Where gaps were found worked with the team to close the gaps. Wrote the Risk Management Plan and performed the Risk Assessment documenting the risks in the risk register. Wrote the required documents for ISO which included the Scope document, the Statement of Applicability, Risk Management Plan, Risk Register, and the overarching Information Security Policy for the Information Security Management System (ISMS). Manager (FTE) Security and Compliance June 2017 to October 2017 Datto Data Backup and Storage company. Reporting to the CISO, brought on to bring the company into compliance in order to assess against SOC 2 Trusted Services Principles, PCI, CJIS and GDPR. Worked with external assessor to complete SOC 2 Type II assessment. Compliance activities involved projects

to implement a security awareness and training program, vulnerability scanning and remediation, implement firewalls and IDS, improve security event monitoring using ELK, reviewing security policies and BCP plans to ensure compliance requirements are covered, perform account reviews, develop asset inventory, and a variety of other tasks to improve overall security program. Worked with Sales to answer client questions about security controls and compliance, and responded to clients' vendor due diligence questionnaires. GRC Manager (FTE) Frontier Communications January 2016 to December 2016 A fortune 500 telecommunications company. Reporting to the VP of IT Security, managed a team of five responsible for Enterprise Governance, Risk and Compliance. Wrote and enforced security policies; produced and delivered security awareness training. Performed risk and security control gap assessments, and coordinated with internal audit; worked with the various departments to remediate to findings. Conducted vendor security reviews, responses to RFPs and business partner security questionnaires/audits, and working with legal team to write data protection and security clauses in contracts and MSAs. Performing annual PCI assessment and filings with card brands and acquiring bank. Worked with Legal, HR, and Physical Security on investigations, legal holds, eDiscovery, and forensics. Reviewed vulnerability scanning, application scanning, and penetration testing reports, then worked with system and application owners to remediate findings. Worked closely with the PMO by attending project status and architectural review board meetings to identify security flaws and weaknesses in new implementations or significant changes to existing applications. Used Archer GRC tool to document assessments, risk register and remediation plans, and store evidentiary artifacts. Documented the Incident Response Plan and handled numerous security incidents. Managed direct reports - performance reviews, time and expense reporting, time-off, handling any matters needing escalation. Mentored and provided educational opportunities to increase skills. Information Security Consultant Independent October 2012 to September 2015 Contracted out to companies needing information security, risk management, and auditing consulting services. Worked with various companies on project to implement controls to improve their security and compliance posture. Performing risk assessments of business critical applications as part of periodic review

process. Developed and information security programs by identifying and prioritizing initiatives and then working with vendors to define ideal solution sets for the client. Wrote information security policies and procedures. Prepared clients for assessments by 3rd party auditing firms and penetration testers. Developed security awareness training programs Managed vendors and projects associated with new implementation of security controls and assisted with design of the security architecture applying multi-tiered, segmented, multi-DMZ network for the new data center. Managed annual pen testing and vulnerability scan results/finding from FY 2013 and managed vendor solicitation and SOW submissions for retesting remediated items and testing for FY 2014. Improved monitoring and incident response capabilities, enhancing use of the SIEM, developing procedures for malware response, and training Security Operations Center staff on effective incident handling processes, as well as proper evidence collection procedures. Implemented vulnerability scanning tools, network monitoring and intrusion detection solutions. Answered client due diligence security questionnaires and performed vendor management. Wrote the Disaster Recovery Plans. Developed vulnerability/patch management processes with metrics to measure continuous improvement. Performed SOX, PCI, and FTC audits, and helped a company achieve ISO 27001 re-certification. Worked with operations teams - networking, server, and applications to remediate security vulnerabilities and correct security parameter misconfigurations to better secure the environment. Developed configuration standards for major system components. INFORMATION SYSTEMS SECURITY OFFICER (FTE) CGI/CGI Federal March 2011 to October 2012 A global leader in information technology offering cloud infrastructure (IaaS) and security services to the Federal Government. Responsible for ensuring CGI's Federal Infrastructure as a Service Cloud services built upon VMware was in adherence to the US Federal Government's security requirements. Prepared documentation for submission package to the FedRAMP Joint Authorization Board (JAB) to take CGI through the FedRAMP C&A process. Worked through the GSA Certification and Accreditation process, building/revising the Systems Security Plan (SSP), Security Assessment Report (SAR), and remediating audit findings tracked and documented in the Plan of Action & Milestones (POA&M) resulting in CGI being the first provider to achieve Authority to

Operate (ATO) from GSA. Developed and enforced security policies related to Personnel Security and Access Control, ensuring support staff obtained appropriate clearances and permissions based on functional roles. Drove security evolution of the infrastructure and tenant environments during both IaaS Cloud Phase I and Phase II projects to improve customer experience of the IaaS Cloud performing risk assessments of architectural designs. Wrote Security Assessment Reports, Configuration Management Plan, and Incident Response Plans. Directed a team of 6 SOC Analysts and 2 Security Engineers to effectively implement security controls and led team through handling of security incidents. Performed security analysis of vulnerability assessments, reviewed/approved access and change requests, user account reviews with annual attestation, lead/oversaw and documented security incident handling with the security operations center. Used various security tools - ArcSight SIEM, SourceFire IPS, Splunk/Syslog-NG/Snare for event monitoring, eDiscovery, Host-based IDS, Active Directory audit reporting, BMC Remedy/ITSM, BladeLogic for Configuration Management and Patching. Information Security Consultant Independent January 2010 to March 2011 Contracted out to companies needing information security, risk management, and auditing consulting services. Worked with a local utility company to develop a risk and vulnerability management program and create an incident response plan prior to a NERC CIP audit. Performed testing of the incident response plan, evaluating lessons learned and improving the plan to enhance communications and procedures for quicker recovery from the effects of the incident. Worked with the security operations team to establish vulnerability scanning and developed metrics reports. Used Archer GRC tool, to document risks, security exceptions, security incidents, policies, standards and control procedures. Performed various security functions including performing regulatory compliance checking against FERPA, FTC Red Flag Rules, HIPAA; performing vulnerability assessments, developing and delivering security awareness training; documenting processes and procedures for access control; incident response, threat monitoring and implementing DLP using McAfee's product. COMPLIANCE MANAGER (FTE) Charles Schwab & Co., Inc August 2008 to December 2009 A financial services and investment company. Built a compliance monitoring and reporting program to ensure technology services

groups across the firm are adhering to policy, standards, and industry regulatory requirements. Responsible for developing or managing: Metrics Reporting, to include building management level dashboards to show effectiveness of security controls. Processing and approving information security exceptions and tracking remediation action plans to achieve compliance. Developing or improving information security standards as a member of the information security governance team.

Served as a consultant for matters relating to policy compliance and implementation of security controls. Performed assessments of vulnerabilities, including zero-day, to quickly determine the impact to the firm, led the effort to mitigate, and documented reports to executive management. INDEPENDENT IT SECURITY/RISK MANAGEMENT CONSULTANT Independent June 2007 to August 2008 Contracted out to companies needing information security, risk management, and auditing consulting services. Implemented an Information Security Program developing policies and standards according to ISO/27002/ Developed incident response program; created risk management program and documented the process. Led external audits and performed internal IT audits in accordance with Government Auditing Standards. Worked with application development team to build security into the Systems Development Lifecycle. Performed security architectural reviews of new system design and implementation plans. Led the compliance team in remediating gaps found in PCI and SOX audits. Assisted with the network infrastructure improvement program, making recommendations for secure system design to adequately protect data via encryption (at rest and in motion). Worked with a CIO to develop the Information Security Program; implementing and operating security controls and developing projects to address security weaknesses. Improved data protection and privacy for persons by implementing Data Governance and setting requirements. Developed a solution for equipping sheriff patrol cars with hardened, secure laptops; to allow secure remote criminal records database access. Created the incident response plan with forensics procedures for electronic evidence collection and handling; led forensics teams during several investigations. Worked with County Health to ensure security and privacy requirements for HIPAA were being met. SECURITY SALES SPECIALIST/SENIOR RISK MANAGER (FTE) Verizon Business August 2005 to June 2007 A major telecommunications with a

business unit focused on delivering managed security services and professional security services. Supported Verizon customers by providing "CISO in a Box" Services, as well as Information System Assessment Services such as Security Program and Policy Development, Regulatory Compliance Audits, Risk Assessments, Penetration Testing, Remediation, and Awareness/Education. Wrote Statements of Work and Proposal responses to RFPs, developed assessment Project Plans, wrote reports of assessment findings, and presented to client executive management. Created and implemented an assessment and remediation program for bringing a large food company into Payment Card Industry (PCI) compliance at each of its stores nation-wide. Worked with a California City on Policy Development to meet regulatory compliance by documenting their security controls, identifying gaps, and implemented an encryption solution for data protection and privacy. Reviewed and rewrote a State Governments information security policies. As Security Sales Specialist sold MCI/Verizon security services to large companies within the financial services sector. IT SECURITY ENGAGEMENT MANAGER (FTE) Jefferson Wells International November 2003 to August 2005 Professional services firm offering internal audit, technology risk management, tax, finance, and accounting services. Led teams during extensive compliance requirements reviews that included the analysis of existing security policies and standards and technical controls, followed by recommendations and implementations of security solutions. For several clients, directed the implementation of Sarbanes Oxley (SOX) controls over change management, database security, secure data processing, Software Development Life Cycle processes, Microsoft Server configuration standards and base-lining for a national educational institution. Conducted Sox 404 (IT General Computing Controls) internal audits for various clients to identify security weaknesses and deficiencies, and then assisted with remediation efforts through the documentation of policy, standards and processes; and then tested processes against IT general and application controls. Assessed control objective effectiveness and control activities for SOX audits utilizing COSO and Cobit frameworks. As a Sales Engineer provided technical support to sales representatives selling JWI services to prospects. ELECTRONIC WARFARE SIGINT ANALYST (98C) United States Army 1983 to 1991 Assigned to the Intelligence and Security Command (INSCOM at the NSA)

Responsible for the collection, analysis, and reporting of foreign intelligence data and received numerous rewards for the handling of significant military intelligence events. As a Staff Sergeant, managed a team of 9 highly specialized senior NCOs. Education Bachelor of Science in Computer Science University of Maryland 1991 Master's in Information Security George Mason University Certification in National Security Agency National Cryptologic School Skills SECURITY (10+ years), INFORMATION SECURITY (8 years), AUDITS (8 years), INCIDENT RESPONSE (7 years), PAYMENT CARD INDUSTRY (7 years), Cissp, Cybersecurity, Information Assurance, Cyber Security, It Security, Nist, Siem, Network Security, Linux, PCI, Cisa Military Service Branch: United States Army Rank: Staff Sergeant, E-6 Certifications/Licenses CISSP May 2003 to May 2021 CISA January 2004 to January 2019 CISM January 2005 to January 2019 Additional Information KEY COMPETENCIES Information Security Program Management Policies, Standards & Regulatory Compliance Security Controls (Firewalls, IDS/IPS, DLP, SEIM) Data Classification, Protection, & Encryption IT Audits (PCI, SOX, GLBA, HIPAA, SOC 2, FedRAMP) Control Frameworks (ITIL, ISO27001/2, NIST) General Data Protection Regulation (GDPR) Risk Management and Risk Assessments Vulnerability and Patch Management Process Documentation & Improvement Disaster Recovery and Incident Response Plans Audit Methodologies and Standards SELECTED FOCUS AREAS: ? Leader in managing Information System Audits for SOX, SOC 2, PCI, HIPAA/HITECH, ISO, NIST, FedRAMP, GAPP and GDPR; developing project remediation plans, driving closure to control gap findings, and achieving compliance. ? Developed Information System Security and Compliance Programs; IT Policies, Standards and Procedures' Risk Management, Change Management; Incident Response, Vulnerability Management; and Disaster Recovery & Business Continuity plans.

Name: Adam Cannon

Email: sanchezthomas@example.com

Phone: (608)762-2298x404