

Senior Global Cloud Ops Compliance and Audit Senior Global Cloud Ops Compliance and Audit

Senior Global Cloud Ops Compliance and Audit - Deltek, Inc Monument, CO Leveraging my 12+ years of Sr. Security Analyst and IT Security Regulatory Auditor. Experience and knowledge in security compliance, internal IT audit of networks and 3rd party associate audits accomplished for Health Care, Fortune 500 companies, Financial Institutions, Oil & Gas, Software as a Service and Federal entities. Following standards of NIST, HIPAA, SCADA, GRC, SOC - SSAE, PCI DSS, PII, SOX and Best Practices; encompasses the understanding of FISMA, FIPS, Risk Management Framework, OWASP threat modeling, Data Privacy, SIG7, ISO 27001/2 application controls - processes. Progressively expanded my skill-set and proficiency by taking on various projects. Committed to these projects with integrity - reliability; seeing them through to complete. Open to a full-time Remote role where my experience and interpersonal skills can bring value. Authorized to work in the US for any employer Work Experience Senior Global Cloud Ops Compliance and Audit Deltek, Inc - Herndon, VA June 2018 to Present Key Results: Met timelines for rolling SOC Audits, multiple NIST Plan development and NIST Compliance reviews; ensured continuous monitoring of privileged access accounts access was reduced by 40+% Conduct security control assessments for compliance to various regulations (SSAE 18 of SOC 1, SOC 2 SOC 3 rolling audits; NIST 800-171, 800-53, FedRamp; ISO 27001; familiar with GDPR and ITAR) for 17 Soft as a Service (SaaS) products. Cloud platforms of AWS, Azure and SoftLayer (IBM Cloud). Develop required security documentation to support compliance. Administer monthly and quarterly reviews to ensure systems are operated, maintained, on-boarded and disposed of in accordance with internal security policies and practices outlined in the security plan. To include on-going access control reviews. Document results of security assessments and recommend technical and analytical guidance to address findings. Report to Information Security management concerning residual risk, vulnerabilities and other security exposures, including misuse of information assets and noncompliance. Sr. Security & Compliance Consultant TechOne Staffing, Inc - Greenwood Village, CO February 2017 to June 2018 Duration: Feb 2017 - June 2018 Key Results: Completed audit of applications ahead of timeline creating a savings of project dollars Scheduled and implemented

IT security audits with system owners using NIST 800-66 for HIPAA and NIST 800-53, NIST 800-53a and NIST 800-37 for baseline assessments. Defined the boundaries of applications / infrastructure, network diagram reviews (Visio) and gathers evidence to support the identified NIST Controls are in compliance with IBM. IT Security Compliance & Audit Consultant PROJECT CONSULTING June 2007 to June 2018 Projects completed for contract agencies for multiple assignments as listed below: Sr. Analyst Vendor Information Security Oversight Randstad Technologies, LP - Lone Tree, CO August 2016 to February 2017 Duration: Aug 2016 - Feb 2017 Key Results: Completed assessments of 3rd party vendors one month early creating a savings of project dollars Conducted vendor third party financial control assessments - GRC; identified vendor gaps / deficiencies; requirements were met for State and Federal Reserve regulations - NIST 800-53a & 800-37, PCI DSS, SOC, ISO and Best Practices. Responsible subject matter expert on financial services of vendor cyber security risk to include risk identification, quantification, and management efforts. Assessed (QA) remediation plans and non-compliance acceptances. Validated evidence from third parties to assist in closing identified findings. Tracked in RSA Archer. Sr. Security & Compliance Business Consultant Rose International - Greenwood Village, CO April 2015 to August 2016 Duration: April 2015 - Aug 2016 Key Results: Completed audit of applications ahead of timeline creating a savings of project dollars Risk profiling of medical clinical devices and applications for IT governance and life cycle for HIPAA, PHI, ePHI, PII, PCI DSS, SOC, SOX, FDA and Best Practice. Performed IT security assessments of networks (IBM RACF, Cloud), Security Operations assets, Facility Operations assets and medical equipment with clients and vendors. Gathered and documented assessment results; a liaison - Point Of Contact with business unit directors, managers and clients; conducted one-on-one meetings with the asset owners. IT Security Compliance & Audit Consultant In Transition February 2015 to April 2015 Completed contracted project. Moved to Denver, CO. Passed Cybersecurity certification. Collaborated with ISACA on their certification program for Cybersecurity Nexus (CSX) III. Contract work for Hewlett-Packard Third Party Global Cyber Security (GCS) Assessment - Houston, TX July 2014 to February 2015 Key Results: Completed required assessments of 3rd party vendors early creating a

savings of project dollars and streamlined team members required for assessments Annual audit of supporting documents - papers for security governance compliance of vendors and business partners. Tracked assessments in the RSA Archer for HP Global. Reviewed regulatory requirements and contractual compliance requirements across multiple industries for Data & Network Security and Privacy. Assessed to security standards - SIG7, NIST 800-53a & 800-37, GRC, SOC, PCI DSS, SOX, ISO/IEC 27001/2, Safe Harbor, EU Data Protection Directive of GDPR - General Data Protection Regulation Security Compliance and/or Best Practice. Sr. IT & Cyber Security Consultant W-Industries - Houston, TX October 2013 to July 2014 Key Results: Mitigated regulatory risks by creating and maintaining operational processes and procedures to ensure compliance with company and regulatory policy and standards Contracted to Energy Transfer Inc. to validate big three external audit findings and assess their IT security policies and procedures posture for their oil and gas enterprise systems and automated industrial control systems (ICS / SCADA). Collaborated with external auditors. Oversaw the creation - draft, enhancement, and adoption of information security policies and standards with the needs of business segments. (NIST 800-53, 800-82 & 800-37, ISO/IEC 27001/2, PCI DSS, CSC SANS Top 20 - CIS Critical Security Controls, INGAA). Contracted to consult with INGAA (Interstate Natural Gas Association of America), defining how the NIST Cyber Security Framework would enhance their cyber security programs. Sr. System IT Security Engineer MRI Technologies - Clear Lake City, TX July 2012 to October 2013 Key Results: Mitigated regulatory risks by creating and maintaining operational processes and procedures to ensure compliance with company policy and standards Sub-contracted to Raytheon at NASA. Provided security compliance validation and implementation for the Neutral Buoyancy Laboratory and the Space Vehicle Mock-up Facility of the International Space Station (ISS) industrial control systems (ICS) that utilizes Rockwell Automation software following ICS SCADA controls in NIST 800-82 and 800-53a. Implemented and maintained IT security procedures, policies and risk reports. Performed vulnerability scans for continuous monitoring using McAfee Foundstone. IT Security Compliance & Audit Consultant In Transition April 2012 to July 2012 Cloud computing, reviewing the newest revision NIST 800-53. Sr. Network

Security Engineer Brandon Technology Consulting - Alexandria, VA January 2012 to April 2012 Key Results: Insured compliance to meet regulatory compliance for NIST and HIPAA, PCI Implemented IT Security Test Plans (Nessus) and Risk Assessment Reports of the DHHQ TRICARE systems for HIPAA, PCI DSS, DIACAP and FISMA / NIST requirements. Utilized the Defense Information Systems Agency (DISA) approved checklists. Reviewed scans of servers, workstations and network equipment configurations. Sr. Information Assurance Engineer NCI Information Systems - Col Springs, CO September 2011 to January 2012 Duration: Sept 2011 - Jan 2012 Security advisor to provide IT network support staff; director level; guidance and clarification.

Technical Subject Matter Expert (SME) tasked with reviewing and drafting operational guidance. Advised government officials on IT compliance to DoD and Federal regulations. Sr. Computer Security & Information Protection Specialist Yoh, Inc - Colorado Springs, CO September 2010 to September 2011 Duration: Sept 2010 - Sept 2011 Provided oversight for IT security. Developed consistent policies and processes of disaster recovery plans and business continuity plans of the individual GPS (Global Positioning System) sites. Interfaced with the appropriate government agencies, customers, and company personnel to facilitate implementation of protective mechanisms and to ensure the understanding of. IT Security Compliance & Audit Consultant In Transition June 2010 to September 2010 Government funding cut and contract slot was eliminated for last position. Moved back to Colorado. Studying for the CISM and CRISC. Keeping up to date on the latest NIST 800-53. Sr. Systems Analyst Yoh, Inc - North Charleston, SC April 2010 to June 2010 Sub-Contracted to SAIC to provide Information Assurance Certification and Accreditation (C&A) and Cross Domain Solution (CDS) support to the Navy at SPAWAR. Provided engineering, integration, technical and administration support for both ship and shore locations. Review of Visio network designs. Sr. Systems Security Engineer Booz Allen Hamilton - North Charleston, SC December 2009 to April 2010 Accomplished NIST and PCI DSS (Payment Card Industry Data Security Standard) compliance verification audits for the US Department of Veterans Affairs (VA). Reviewed risk assessment reports for senior executives; quantifying and verifying plans to remediate; evaluated compliance closures for National Science Foundation (NSF) Antarctica. Sr.

C&A Security Analyst G&B Solutions - Lakewood, CO December 2008 to December 2009 FISMA / NIST 800-53a auditing, FIPS 199 & NIST 800-37, SSAE assessments; interviewed key organizational personnel; updated reporting of eMASS state; composed risk reports. Conducted in-depth technical reviews of new and existing IT systems (Windows, UNIX, RACF) for compliance with policy and industry guidelines for the DOI and the Department of Transportation (DOT) for ongoing monitoring of IT security controls. Sr. Systems Security Engineer Boecore - Schriever AFB, CO December 2007 to December 2008 Contracted to Northrop Grumman Mission Systems to provide technical IT Security expertise in Information Assurance for compliance support of classified and unclassified systems. Provided technical security engineering support for complex software, hardware, network systems; design, develop, and execute security tests and evaluations (ST&E) of annual audit plan, vulnerability assessments and audits; risk mitigation and analysis of security threats. Education A.A. in General Studies University of Maryland 1992 A.A.S. in Electronic Systems Technology Community College of the Air Force 1990 Skills Auditing (10+ years), IT SECURITY (10+ years), BUSINESS CONTINUITY - DISASTER RECOVERY (10+ years), CISA (8 years), CISM (8 years), Regulatory Compliance (10+ years), NIST FISMA FIPS (10+ years), Security Risk Assessment & Management (10+ years), Policy Management & Compliance (10+ years) Links <http://www.linkedin.com/in/marilyn-sousa-cisa-cism> Military Service Branch: United States Air Force Rank: E-6 Certifications/Licenses Certified Information Systems Auditor (CISA) March 2010 to Present

<http://www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/What-is-CISA/Pages/default.aspx> Certified Information Security Manager (CISM) June 2011 to Present <http://www.isaca.org/Certification/CISM-Certified-Information-Security-Manager/What-is-CISM/Pages/default.aspx>

Name: Lisa Gibson

Email: ernestmartin@example.org

Phone: 466-618-8315x072