SR. INFOSEC GRC ANALYST SR. INFOSEC GRC ANALYST SR. INFOSEC GRC ANALYST - ExamWorks, Inc Atlanta, GA Work Experience SR. INFOSEC GRC ANALYST ExamWorks, Inc - Atlanta, GA 2016 to Present * Facilitates HITRUST, SOC2 audit engagement, data/artifact collection, exception remediation, and monitoring * Completes and processes 160 client security questionnaires from multiple business units (BU) annually into Excel spreadsheet. * Conduct third-party vendor risk assessments using Third Party Trust's GRC tool. * Traveled to meet with business unit leaders to understand processes and procedures of the BU * Collaborates with teams across the organization to develop and execute the information security management program framework * Identifies potential security vulnerabilities during the design stage of technical solution development * Performs cybersecurity analysis, correlation, and prioritization of findings discovered in scans and vendor bulletins * Monitors vendor and cybersecurity notices and reports to develop security advisories to distribute out to the business * Understands, develops, adheres to, and implements overall cybersecurity and configuration policies/procedures in alignment with industry standard security compliance frameworks such as HIPAA, HITRUST, ISO 27001 * Contribute to the design, implementation, and optimization the GRC application or solutions * Identifies critical tasks necessary to remediate risks including operational, regulatory, and industry standards * Analyzes and resolved issues of minimal to moderate complexity including network and security operations, firewall administration, systems administration, server operations, applications support and project management * Prepares analytical reports for both services and performance; allocates internal and external IT resources to support demand effectively * Provides security recommendations to internal project teams to enable teams to make informed decisions * Research and design appropriate IT controls to provide a secure environment; utilizing various IT frameworks and standards including ISO-27001, NIST, and COBIT * Assists in the substantive testing for employee access review, provisioning, terminations, and change management practices for all critical changes (applications, operating systems, servers, and databases) * Maintains current knowledge and emphasis on HIPAA and HITRUST assessment related to data confidentiality * Maintained and tracked an inventory of all open audit (internal/external), assessment, and other third-party findings in addition to exceptions to policies and standards * Provided support and contributed to the company's IT GRC programs such as risk management, third-party/vendor management, vulnerability/threat management/compliance management/request for proposal, and security assessment questionnaire process management IT SECURITY ANALYST, THIRD-PARTY RISK ASSESSMENT Diversant, LLC - Atlanta, GA 2015 to 2016 * Built & maintained relationships with internal business partners and third-party points of contact to gather information on the services the third-party provided and determined the risk the services may have posed to the company * Conducted remote assessments using a NIST and PCI framework-based questionnaire * Led initial and, if necessary, follow up interviews with third-parties, collected and examined third-party documentation including SOC 2 types I and II, ISO 27001, and PCI DSS AOC Attestation reports to determine compliance with control domains CYBER RISK ASSOCIATE Deloitte, LLC - Atlanta, GA 2015 to 2015 * Traveled to client sites to interview stakeholders to determine if security controls were being implemented * Inspected evidence and documented findings during the assessment * Sent follow up emails requesting evidence; completed findings report, made recommendations, participated in practice development projects, completed job-related and other training; other duties as assigned IT SECURITY ASSOCIATE VariQ 2014 to 2015 * Provided support to plan, coordinate, and implement the organization's information security * Facilitated and helped agencies identify their current security infrastructure and define future programs, design, and implementation of security related to IT systems * Provided technical input related to FISMA issues to more senior security specialist and, when required, provided technical input to the IRS FISMA reporting team * Provided highly technical and specialized guidance, and solutions to complex security problems * Performed analyses and studies; prepared reports and gave presentations to management * Attended various stakeholders' meetings including control selection, ad hoc, control assessment, participated in weekly staff meetings, and trainings offered both onsite and remote CYBER RISK ASSOCIATE, Federal Government Contractor L-3 Stratis - Greenbelt, MD 2012 to 2014 at NASA Goddard Space Flight Center * Used NIST Special Publication 800-53 and FISMA guidelines to determine subsystem Plan of Action and Milestones (POAMs) and entering them into the compliance platform Risk Management System (RMS). * Managed inventory, secure configurations, system boundary and scope, audit logging checks, Elevated Privileges Management and Access Control, Vulnerability Management, Security Plan Review. * Made hardware purchasing decisions, monitored server and workstation backups using Backup & Restore Utility (BRU) and rotated backup tapes daily. * Played integral role in the preparation of yearly system assessments, including current system data, preparing audit spreadsheet, gathering system and procedural documentation from administrators, participating in inbrief/outbrief process at both on- and off-site locations; other duties as assigned   Additional Work L-3 Stratis, Technical Specialist, Suitland, MD L-3 Stratis, Systems Security Analyst, Greenbelt MD Education Bachelor of Science in Computer Networking Strayer University October 2019 Skills Microsoft Office Links http://www.linkedin.com/in/stephanie-smallwood Certifications/Licenses ITIL Foundations v3 February 2013 to Present CRISC-Candidate October 2019

Name: Renee Barber

Email: zjensen@example.com

Phone: 706.863.2816x0010