Information Security Risk Analyst Information Security Risk Analyst Information Security Risk Analyst - Medstar Washington Hospital Center Dumfries, VA Interactive, flexible and quick-thinking Information Security Analyst with the ability to study and learn new context expeditiously seeking to join a growth oriented company with innovative initiatives. Authorized to work in the US for any employer Work Experience Information Security Risk Analyst Medstar Washington Hospital Center October 2017 to Present Performs Vendor/3rd Party Security Risk Assessment to assess the effectiveness of cloud vendor's controls against ISO 27001, HIPAA, and NIST 800-53rev4. Perform Internal Security Risk Assessments with a focus on existing and new systems for business units. Conducts risk assessments by review security documentations, policies, SOPs, in line with the Hospitals policies and procedures. Create Security Assessment reports, identify gaps and track remediation activities. Review and Analyze SOC 2 Type II reports of 3rd parties and Data Centers. Engaged in Regulatory Security Risk Assessments and audits for effective compliance with HIPAA. Engaged in tracking security incidents and conducting risk assessment on service request. Developed System Security Plan (SSP), Security Assessment Report (SAR) and POA&Ms. Assisted in the development of key security standards and guidelines by performing an in-depth security assessment for HIPAA, Security and Breach Notification Rule compliance evaluations, ISO 27001 and SOX to help gain compliance. Creates and executes repeatable work processes and procedures; with excellent verbal and written communication updates security documents such as policies, standards, and operational procedures. IT Security Analyst New York University Langone Medical Center September 2015 to August 2017 Performed Vendor Risk Assessment to assess the effectiveness of vendor's controls against ISO 27001, HIPAA, HITECH, and Meaningful Use requirements through the use of GRC tool Monitored and reports on compliance with information security policies, standards, procedures and guidelines. Conducted risk and security assessments and evaluated results with system owners and custodians. Provided information security consulting on a variety of technologies and processes. Works with clinical, academic, and administrative groups to develop security solutions with minimum supervision. Supported and helped numerous activities related to risk assessments. Performed risk assessment on information assets including: information systems, biomedical systems, clinics, vendors and data centers. Performs Risk Assessment for NYULMC data centers, departments, applications etc. using NIST 800 - 53 rev 4 controls with Archer GRC. Developed new and improves upon existing information security risk assessment methodologies. Identifying security threats, attack methodologies, security principles, best practices, and evasion techniques. Participates in annual review of all information security policies, standards, procedures and guidelines; recommends new policies and amendments; assures alignment with current regulatory requirements. IT Security Risk Analyst T. Rowe Price August 2013 to August 2015 Worked with Information Security team to develop and maintain a security plan Worked closely with IT groups, business units to ensure security policies and procedures are adhered to. Worked with auditors and third party assessors on risk assessments, penetration tests and vulnerability assessments. Assessing control gaps and auditing applications within the organization. Developed report after audit findings, remediation, perform gap analysis and a corrective action plan in accordance to the organization's policy. Conducted risk assessment on new systems for business units within the company Monitored all in-place security solutions for efficient and appropriate operations Experience in information security policies, standards, industry best practices, and frameworks(ISO 27K, PCI DSS, NIST 800-53, FISMA, etc) Coordinated with stakeholders to initiate, scope and plan controls assessments of new and existing vendor engagements. Education Master of Science in Cyber Security and Information Assurance Virginia Commonwealth University Skills Nist, Security, Risk assessment, Soc, Satisfaction Additional Information Special Skills: Efficient in planning, project set-up, project management and providing support for assigned engagements. Project Setup and customization using Archer GRC Review and Analyze SOC 2 type II reports. Security categorization and assist in selection of Technical, Operational and Managerial controls using FIPS 199 process and NIST SP 800-60 guidelines. Review and update Risk Assessment (RA) using NIST SP 800-30 guidelines Create POA&M to take corrective actions resulting from vulnerability scanning, compliance check and system test and evaluation (ST&E). Excellent analytic and problem-solving skills, especially in the information systems, security and/or privacy space. Have the flexibility to multi-task and prioritize work load, work independently or share workloads and deal with sudden shifts in project priorities. Effective communication skills to build and maintain customer satisfaction and express opinions in clear sound manners on matters associated with IT security.

Name: Michael White

Email: woodsjonathon@example.com

Phone: 751.231.7545x11320