IT SECURITY ANALYST IT SECURITY ANALYST CYBER SECURITY ANALYST Sayreville, NJ IT Security professional with over 5 years of experience specialized in Security Assesment & Authorization (SA&A), Cybersecurity, Risk Management, System continuous monitoring, Regulatory compliance, Vulnerability Management, and project management. Expertise in FISMA compliance Work Experience IT SECURITY ANALYST ROBERT WOOD JOHNSON UNIVERSITY HOSPITAL June 2018 to Present -Responsible for the development of key security standards by performing in-depth security assessment of RWJUH information systems in order to maintain in HIPAA compliance by implementing guidelines and standards identified in National institute of standards and technology 800-66 (NIST SP 800-66) -Conduct IT control risk assessments that includes reviewing organizational policies, standards and procedures and provide advice on their adequacy, accuracy and compliance with the PCI DSS standard. -Business Impact Analysis (BIA) to analyze mission-critical business functions and Identify and quantify the impact if there is loss (operational, financial). BIA helps to define the company's business continuity plan and IT internal control audit objective. -Performed IT general control audits (ITGC) in relation to Sarbanes Oxyley (SOX) section 404 framework. -Analyze discovered infrastructure and software vulnerabilities obtained from scanning to determine risk, impact and remediation strategies -Manually reviewed logs and provided documentation guidelines to business process owners and management. -Review contingency plan and disaster recovery operation policy and procedures for compliance -Performed maintenance and advanced configuration of systems order to protect systems from emerging cyber threats. -Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. -Perform vulnerability assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the information and information systems. IT SECURITY ANALYST NEW YORK SPORTS CLUB September 2017 to April 2018 -Analyze and update system security plan (SSP), risk assessment (RA), Privacy impact assessment, system security test and evaluation and the plan of actions and milestones. -Conduct IT controls risk assessment that included reviewing organizational policies, standards and procedures and provided advice on their

adequacy, accuracy and compliance with the payment card industry data security standard. -Asses system design and security posture as well as advise information security compliance with FISMA and NIST SP 800-53 rev4 controls. -Develop security baseline controls and test plans used to assess implemented security controls. -Create Security Assessment Reports (SAR) identifying the results of the assessment along with the Plan of Action and Milestone (POAM) -Conduct interviews, test and examine organizational processes and policies for FISMA compliance -Conduct follow up meetings to assist ISSOs, System owners and Authorizing officials to close remediated POA&M items. -Perform and recommend maintenance and system configuration settings in order to protect systems from emerging cyber threats. -Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages. FISMA/C&A ANALYST STAPLES December 2016 to July 2017 -Analyze and update system security plan, risk assessment, privacy impact assessment, system security test and evaluation and the plan of actions and milestones. -Ensuring that management, technical and operational security controls adhere to a formal and well established security requirements authorized by NIST SP 800-53 -Conduct self-annual assessment. Overall assessment of systems every year to ensure company has complied with security controls and assessment of possible vulnerabilities, as well as ensuring all assessments are accurate. -Conduct IT controls risk assessment that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the payment card industry data security standard. -SOX 404 compliance analyst; that is assessing system design and security posture as well as advice information security compliance with Sarbanes oxyley section 404 framework. -Perform IT risk assessment and document the system security key controls -Meet with IT team to gather evidence, develop test plans, testing procedures and document test results and exceptions -Design and conduct walkthroughs, formulate test plans, test results and develop reeducation plans for each area of the testing -Wrote audit reports for distribution to management and senior management documenting the results of the audit -Develop a business continuity plan and

relationship with outsourced vendors -Evaluate clients' key IT processes such as change management, systems development IT SECURITY ANALYST Iron Mountain Data center May 2016 to November 2016 -Conduct security control assessment for new client systems based on NIST SP 800 53 A Rev4 and in accordance with client policies and procedures. -Leadership in utilizing Risk Management Framework (RMF) process to enable successful approval to operate (ATO) -Ensure that security policies, procedures, and recommendations comply with NIST, FISMA organizational guidelines and technical practice. -Analyze discovered infrastructure (physical) and software vulnerabilities obtained from scanning to determine risk, impact and remediation strategies. -Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. -Conducted a vendor security assessment on systems applying the steps and procedures of the SSAE 18 framework. -Develop System Security Plan (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements. -Assist system owners and ISSO in preparing certification and accreditation packages for companies IT system, making sure that management, operational and technical security controls adhere to a formal and well established security requirement authorized by NIST SP 800-53 Rev 4 Education Bachelor of Science in information technology University of Ghana 2014 Skills Information Security, Cyber Security, It Security

Name: Tommy Vega

Email: kellyyvonne@example.org

Phone: +1-418-687-3302x354