Information Security Analyst Information Security Analyst Information Security Analyst - New York Presbyterian Hospital Extensive years of experience in Information Security system assessment, C&A and Risk Assessment of General Support Systems (GSS). Specialized in regulatory compliance standards and frameworks like HIPAA, SOX, GLBA, ISO and FISMA. Seeking for opportunities as IT Security Analyst in an organization with focus on Information Assurance, HIPPA Compliance Assessment and internal controls Audit Engagements, Risk Assessments, Certification and Accreditation (C&A). Work Experience Information Security Analyst New York Presbyterian Hospital - Queens, NY April 2013 to Present Develops and enforced HIPPA policies and safeguards procedures in accordance with NIST 800-66. Conducts internal monitoring, auditing and assessments of policies and procedures for necessary amendments. Establishes effective channels for communications for effective employee and management training. Performs Vendor/Third Party Risk Assessment on the effectiveness of vendor's controls against HIPAA, HITECH and ISO 27001 through the use of GRC tool. Keep up-to-date on related regulations and industry best practices. Perform security risk assessments with a focus on existing and new systems, against HIPAA and NIST 800-53Rev4. Engaged in Regulatory Security Risk Assessments and audits. Creates assessment reports and track remediation activities. Coordinates Change Control process. Perform exceptions reviews to ensure processes and technologies for transmitting and storing PHI meet HIPPA security rule requirements. Oversees Vulnerability management process after a scan on the hospital's external and Internal IP addresses. Creates a remediation plan for mitigating findings after every external audit. Performs PCI assessments and analysis of threats and vulnerabilities on vendor applications. Develops remediation plans on PCI-DSS findings and creates reports on compliance (ROC). Assists with documentation of policies, standards and operational processes. Assists with remediation of vulnerabilities findings and ensure they are fixed in a timely manner by engaging personnel involved. Utilizes Service Now and Archer tools for security approval of applications and tracking of third party vendors on compliance. Vendor Risk Analyst Business Interface, LLC - Wilmington, DE June 2012 to March 2013 - Contract Developed a vendor risk program and performed vendor risk

assessments for Business Interface (scorecard, questionnaire, reporting, and monitoring). Coordinated with business units and staff to provide guidance on the process of conducting risk analysis, computer security reviews and security assessments. Keep up-to-date on related regulations and industry best practices and created assessment reports for tracking remediation activities. Ensured that vendors had formal security policies, disaster recovery/pandemic plans and vendor performing security checks across all functionalities. Perform and review risk assessment on security posture of vendors against industry's best security practices and enterprise requirements. Worked with senior managers and assisted on investigative matters, related to information security in ensuring that vendor is maintaining quality standards without causing risks to our data. Developed Vendor Risk Management monitoring tool to ensure all vendors are up to date on contract renewals and risk management reports. Use GRC (Archer) tools to monitor PCI DSS compliance of vendors. IT Security Analyst InTec, LLC - Washington, DC October 2011 to April 2012 - Contract Reviewed, developed and gathered evidence of business and operational systems security which included compliance efforts in support of HIPAA, PCI and ISO 27001. Helped in establishing an information security management system for cross functional teams in improvement efforts for continual service and security service delivery. Provided monitoring and incident management scorecard reporting systems for executive and management review. Provides professional security engineering and compliance efforts according to, GLBA, HIPAA, PCI-DSS regulations in developing security infrastructure. Developed Security Test Plan (STP) and Security Assessment Report (SAR) detailing the results of the assessment along with Plan of Action and Milestones (POA&M) Conducted kick off meetings to collect systems information (information type, boundary, inventory, etc.) and categorize systems based on NIST SP 800-60. Assisted in the development guidelines and key security standards by performing an in-depth security assessment for HIPAA, PCI DSS, ISO 27001 to help in gaining compliance.

Name: Melissa Walker DDS

Email: amberryan@example.net

Phone: 001-725-569-3443