

IT Security Analyst (Contractor) IT Security Analyst (Contractor) IT Security Analyst (Contractor) - TDCJ - Texas Houston, TX I am an Information Security analyst with 4 years experience in risk assessment and auditing for HIPAA, Sarbanes-Oxley 404, GLBA, ISO, and PCI-DSS reviews. I have experience in C&A - continuous monitoring both major and minor applications. I am involved in developing Risk Management Frameworks, I conduct Vendor Risk Assessments (3rd Party Security Risk Assessment), Certification & Accreditation (C&A) (FISMA) and auditing internal controls using SOX 404 and GLBA and also in HIPAA security assessments. Authorized to work in the US for any employer Work Experience IT Security Analyst (Contractor) TDCJ - Texas June 2018 to Present Support the self-annual security assessment and test security controls based on NIST SP 800-53A. Assist in conducting internal security risk assessments making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4. Review Vulnerability Assessment reports, create POA&M and follow up with remediation processes. Support disaster recovery plan activities and participate in DRP test exercises. Review documents such as security assessment plans, risk assessments reports, Disaster Recovery Plans, and evidences provided on security assessment. Work with vendors to ensure security provisions for applications are requirements with the organization's policies. Perform HIPAA Security Assessment and evaluation to ensure the organizations in compliance with OCR requirements. Information Security Risk Analyst (Contractor) Montefiore Medical Center - New York, NY July 2017 to May 2018 Performed security risk assessments on new and existing systems that affect clinical care, against the HIPAA and HITECH requirements. Performed Vendor Risk (3rd Party Risk Assessment) to assess the effectiveness of vendor's controls against the HIPAA, HITECH, ISO 27001 through the use of GRC tool. Assisted in Regulatory Security Risk Assessments. Completed risk assessments, security requirements analysis, and security testing. Created assessment reports and track remediation activities. Monitored all in-place security solutions for efficient and appropriate operations. Assisted with the documentation of policies, standards, and operational processes. Audited major applications within health systems and assessing control gaps. Assessed security control test plans and

conducted in-depth security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and policies safeguards in order to maintain HIPAA compliance base on Office of Civil Right (OCR) protocol, NIST SP 800-66 Rev1 and security controls (NIST SP 800-53 rev 4). Development of HIPAA compliance reports, documenting auditing findings and development of corrective actions plans. IT Security Analyst (Consultancy) System Security Plan December 2015 to June 2017 Perform IT risk assessment and document the system security keys 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 remediation plans for each area of the testing Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M) Assist System Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct Self-Annual Assessment (NIST SP 800-53A) Conducted I.T controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the PCI DSS. Wrote audit reports for distribution to management and senior management documenting the results of the audit Participate in the SOX and GLBA testing of the Internal Controls. Desktop Support Staff L-Plus Microsystems February 2011 to July 2013 Assisted clients with PC and Desktop Application Issues Regularly performed Software maintenance Trainings on the use of Microsoft Office Applications. Monitored IT threats environment and recommended remediation activities. Education Bachelor's in B.A Arts University of Cape Coast August 2007 to May 2011 Skills Microsoft office (5 years), Information Security, It Security, Security Certifications/Licenses FISMA Compliance Certification Training March 2014 to Present Health Information Technology for Economic and Clinical Health March 2014 to Present

Name: Elizabeth Singleton

Email: hillcatherine@example.com

Phone: 001-395-498-6626