Senior Consultant: Security Analyst Senior Consultant:Security Analyst IT SECURITY SPECIALIST - SIGNATURE CONSULTS Austin, TX ? Ability to maintain and manage the required systems security documentation. These include but not limited to; System Categorization Worksheets (SCW), Privacy Impact Assessments (PIA), Security Control Assessments (SCA), System Security Plans (SSP), Risk Assessments (RA), Contingency Plans (CP) and testing, FIPS 199 Security Categorization, Security Control Test & Evaluation (SCT&E), Certification, Disposition plans, Annual and Quarterly Security Documentation review and testing, ATO certifications and re-certifications, Security Self Assessments (SSA), Memoranda of Understanding (MOU), Interconnection Security Agreement(s) ? Excellent understanding of vulnerabilities/weaknesses across complex IT environments and ability to understand applicability of security standards across technologies. ? A subject matter expert in the field of risk-based Security Assessment and Authorization (A&A) using various State, Federal, DoD, as well as International Cybersecurity frameworks (e.g. NIST RMF, DoD RMF, FedRAMP, DIACAP, HITRUST CSF, HIPAA, PCI DSS, COSO/COBIT, ISO 27001, etc.) ? Ability to record system security plan information in the eGovernance, Risk and Compliance application to promote and develop security strategies; directing system control development and access management, monitoring, control, and evaluation. ? Experience with Risk Management Framework (RMF) and knowledge of the DoD Information Assurance Certification and Accreditation Process (DIACAP). ? understanding and professional knowledge in providing support and guidance to System Owner s through the NIST Risk Management Framework and System Assessment and Authorization processes, including monitoring C&A, self-assessment (NIST 800-53A) completion, vulnerability scans, contingency plan testing, and POA&M management. ? Perform comprehensive Security Control Assessment (SCA) and write reviews of management, operational and technical security controls for audited applications and information systems. ? Ability to evaluate changes or additions to information systems/applications, analyzing potential effects and side effects in advance and assist in vulnerability scanning and remediation efforts for identified security concerns. ? Ability to lead initiatives for internal and external audits, compliance, and regulatory activities, aligning with standard frameworks such as FISMA, ISO 27001/27002, SOC II/Type II, HIPAA, PCI DSS, SOX,

GLBA, FFIEC, EU GDPR, etc. ? Ability to review software application requirements to assure that the applicable security requirements are identified and to determine if they are compliant with security standards. ? Willingness to continue to stay current with relevant Federal and state information security, privacy laws and regulations and modify programs accordingly to remain compliant, as well as consistent with industry best practices. ? Possess strong communication and presentation skills; clearly and concisely express ideas in groups and one-to-one conversations, formal and informal documents. Adapt writing and communications styles to fit the audience. ? Familiar with network devices, configurations and technical security controls. Working knowledge of Cisco routers and switches, firewalls, TCP/IP protocols. Work Experience Senior Consultant: Security Analyst CGI Group - Richmond, VA October 2018 to Present Establish a process to review and update clients IP whitelisting. Identify vulnerabilities and weaknesses in the clients security posture by running Nessus vulnerability scans, identify the associated impact to the Clients systems and recommend remediation actions. Provide actionable threat intelligence to business units that enables proactive threat mitigation strategies and threat-informed decision making and also help maintain effective security countermeasures. Conduct Risk Assessments including 3rd Party Risks, Develop a Risk Register and Risk Treatment Plan for Clients ISMS. Developed a Business Impact Analysis (BIA) which subsequently helped informed a Continuity of Operation documentation. Documented a Disaster recovery plan for current client, including identifying recovery facilities and documentation needed in the event of a disaster. Developed a security Incident Response Plan that helps detect and react to security incident. Assess management controls over client s infrastructure to ensure its Information Technology (IT) is planned, managed and maintained to support efficient operations through security reviews. Provide consultancy on best practices to encrypt sensitive database information and assess the full impact of this modification on client s database. Audit client s current security posture for compliance with CIS top 20 controls and develop plan of action to remediate any defects identified. Help client resolve vulnerabilities and ensure compliance with industry best practices (COV SEC 501, NIST 800-53) using a Statement of Applicability (SOA) Matrix . IT SECURITY SPECIALIST SIGNATURE CONSULTS - Addison, TX

October 2017 to September 2018 Part of the Global Information Security (GIS) controls Governance team responsible for regulatory, Policy and controls mapping. This ensures GIS Control owners understand their regulatory and policy requirements. This process requires using both technical and business knowledge to perform detailed mapping, drive engagement with control owners, and surface potential gaps between GIS controls. * Directly responsible for mapping policies and procedures to assure compliance with applicable regulatory and legal requirements as well as good business practices. * Identify gaps in policies, Identify control owners and forward for remediation. * Identify control owners and which Non-GIS department implements what control. * Review finished mapping documents and convert into archer. SECURITY COMPLIANCE ANALYST IBM - Lansing, MI May 2017 to September 2017 Responsible for documenting security controls from six compliance requirements (HIPAA, FISMA, FEDRAMP, SOC II type II, FIPS 140-2, ISO 27001/2) and assessing policies, and procedures for clients migrating data into AWS. Document security controls for migration team (both Production and Development environments) migrating data into AWS infrastructure for client. Analyzing the effectiveness of compliance activities, and report risks with recommendations to management. Supports development of security related policies and standards for both migration team, the client and Managed Service Provider. Serves as point of contact for IT and information security requests. Develop a working knowledge of the operational processes and controls in place supporting all compliance programs and auditing these controls and processes. Audit Security Controls before UAT. Develop gap analysis to identify gaps and recommend remediation actions. Drive security compliance initiatives to completion in an effective and efficient manner. Develop a RACI document to identify who is Responsible, Accountable, Consulted or Informed about security controls. Identify open issues in previous audit reports and assess updates to the documents with respect to these issues. FISMA ANALYST TEXAS JUVINILE JUSTICE DEPARTMENT February 2014 to April 2017 Conducted / assessed IT systems for compliance in a diverse technology environment across varying infrastructures, applications and networks. As requested assist on investigative matters, related to information security, prepared scheduled FISMA reports, Conduct PO&AM reviews, oversight and reporting and Conduct Privacy

Impact Assessments Documented and managed Risks in accordance with SP 800-30 and SP 800-37 using various steps to evaluate the threats, vulnerabilities, and security controls surrounding the information system as well as the likelihood of an exploit and the impact it will have to the system operations Conducted walkthroughs, formulate test plans, document gaps, test results, and exceptions Participated in the FIPS 199 process using SP 800-60. Certification activities which include Annual Assessment on physical and non-physical assets, Risk Assessments report (RA), System Security Plans (SSP), Contingency Plans (CP), CP Test, Security Assessment Report (SAR), Plan of Action & Milestone (POA&M), certification recommendation, Security Test & Evaluation (ST&E) and Security Evaluation reports that will result in Accreditation of all systems. Requested and reviewed vulnerability scans. Performed a range of IT audit, internal audit, and other related information system services including NIST 800-53 security control assessment. Assisted in process improvement, policy/procedure development, network architecture assessments, IT risk assessments, application control reviews, systems implementation assistance, and a wide variety of other technology related services. Monitored and analyzed Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) to identify security issues for remediation. RISK ANALYST AMERICAN AIRLINES - Fort Worth, TX September 2011 to January 2014 Identified areas that required increased security controls to protect the organization and its end users from future fraud, and coordinate with outside authorities and law enforcement on fraud case inquiries via email, phone and fax, responsible for building and maintaining a strong level of customer service. Helped guide System Owners and ISSOs through the Certification and Accreditation (C&A) process Ensured the management, operational and technical controls for securing either sensitive Security Systems or IT Systems are in place and are followed according to Federal guidelines (NIST SP 800-53) and ISO 27001/2. Supported Systems Test and Evaluation (ST&E) efforts and other support to the IT Security Office Certification and Accreditation Package review per NIST SP 800-37 using the six steps to evaluate the threats, vulnerabilities within the system Conducted system risk assessment through risk analysis, assesses assets within system boundaries, and identifies all people vulnerabilities within the system.

Develop user training and awareness programs on risk and compliance issues regarding information security. Ensure project teams comply with information security policies and procedures by preparing project security plans and conducting periodic internal audits in readiness for our annual SSAE16 audits (type II). Assisted stakeholders across the business in resolving security policy issues, maintaining compliance, and implementing security procedures Documented and finalized Security Assessment Report (SAR). Education M.A in Development Studies University of Ghana September 2018 B. A in Sociology University of Ghana May 2005 Skills Information Security (7 years), Data Security (5 years), Application Security (4 years), Information System Auditing (5 years), Cloud Computing (2 years), Excel (5 years), SIEM (3 years), NIST RMF (7 years) Certifications/Licenses CompTIA Security+ March 2017 to March 2020

Name: Christine Wilson

Email: raymondhannah@example.com

Phone: 001-945-271-4190x1667