IT SECURITY ANALYST IT SECURITY ANALYST IT SECURITY ANALYST - FRONTIER INC Hyattsville, MD Authorized to work in the US for any employer Work Experience IT SECURITY ANALYST FRONTIER INC June 2017 to Present   Expertise in National Institute of Standards and Technology Special Publication (NIST SP) documentation: Performed assessments, POAM Remediation, and document creation using NIST SP 800-53 Rev.2 and NIST SP 800-53 Rev.4 Have in depth experience performing audit with IT general controls (ITGC) such as, access control, change management, IT operations, disaster recovery and platform reviews (Windows and UNIX OS).   Performed audits using COBIT, COSO, PCI DSS, OMB Circular A-123, and FISCAM Frameworks.   Completed Sarbanes-Oxley (SOX) Section 404 testing of critical systems and applications that financially impact the company and communicate with the Company's external auditors on general computer control related matters and SOX test procedures.   Performed Audits over application security involving the Company's ERP systems. (SAP, People Soft, Oracle Financial, Deltek Cost Point, People soft) and execute audit strategy.   Performed SAS 70 (SSAE18) reviews for large clients in the Manufacturing, Energy, Healthcare and Financial industry.

   Conduct Annual Reviews of System Security Plans of CFO Systems.   Provide IT Audit Support and Coordination for the office.   Conduct Annual Assessments of Tested Critical CFO Systems Controls to reduce IT Material Weakness.   Perform IV&V over Components V&V to make sure that the identified deficiency noted on the NFRs have been remediated.   Conduct A-123 control Assessment of components systems.   Drafted Test Procedures for Attachment R controls for CFO designated Systems.   Have in depth experience performing audit with IT general controls (ITGC) such as, access control, change management, IT operations, disaster recovery and platform reviews (Windows and UNIX OS).   Assisted in IT management by identifying gaps between policy and process, developing recommendations to remediate control weaknesses and responsible for developing and maintaining IT control metrics related to compliance activities.   Performed a Quality Assurance (QA) Review over all Sustainment Assessed Controls.   Tested compliance with company policies and procedures to ensure it conforms to industry standards and applications such as ISO and ITIL frameworks. IT SECURITY AUDITOR SCIENTIFIC SYSTEMS & SOFTWARE

INTERNATIONAL March 2013 to May 2017   Planned and coordinated Information Technology Audits. Ensured audit tasks were completed accurately and within established timeframes using application frameworks such as the FISCAM, FISMA, NIST, COBIT, and COSO.   Audited, tested, and implemented Enterprise Resource Planning Software: SAP, Oracle Financials, and PeopleSoft.

  Performed audit tests, compliance tests, and substantive tests, and identified key controls and weak points and mapped them against the COBIT and FISCAM frameworks.   Implemented section 404 and 302 of SOX and tested controls over segregation of duties and change management and worked on the evidence gathering to support the SOX Acts Compliance Program.   Developed expertise in National Institute of Standards and Technology Special Publication (NIST SP) documentation: performed assessments and supported POA&M remediation and document creation using NIST SP 800-53 Rev.4.   Developed knowledge of several computer environments: performed evaluation and provided guidance on security control implementation on multiple environments including Windows Server, Windows 8, Windows XP, Solaris, Oracle, Cisco IOS, custom applications, and COTS applications.   Created security documentation including updates to System Security Plans (SSP), Risk Assessments, Incident Response Plans, and Change Control procedures.   Supported POA&M Remediation by evaluating policies, procedures, security scan results, and system settings in order to address controls that were deemed insufficient during Certification and Accreditation (C&A), RMF, continuous monitoring, and FISCAM audits.   Assisted ISSOs in creating solutions to weaknesses based on system functionality and pre-existing architecture.   Performed Risk Management Framework (RMF) assessments in several different environments using both scanning tools and manual assessment. Assessments included initiating meetings with various System Owners and Information System Security Officers (ISSO), providing guidance around evidence needed for security controls, and documenting findings of the assessment. IT AUDIT SPECIALIST EZEK SYSTEMS LLC - Washington, DC June 2012 to February 2013   Experience with IT general controls such as access control, change management, IT operations, disaster recovery and platform reviews (Window and UNIX OS   Worked with the IT management team to evaluate controls. Perform assessments, monitor regulations, and work with

auditors to ensure company compliance   Have in-depth experience in using COBIT, COSO, PCI DSS, OMB Circular A-123, FISCAM and FISMA frameworks in performing the audit.   Completed Sarbanes-Oxley Section 404 testing of critical systems and applications that financially impact the company and communicate with the Company's external auditors on general computer control related matters and SOX test procedures.   Performed Audits of application security involving the Company's ERP systems. (SAP, People Soft, Oracle Financial, Deltek Cost Point, People soft) and execute audit strategy.   Performed SAS 70 (SSAE18) reviews for large clients in the Manufacturing, Energy, Healthcare and Financial industry.   Evaluate effectiveness of control activities in order to provide reasonable assurance regarding client's achievement of their business objectives including, accounts payable, accounts receivable and cash disbursements   Assist in IT management by identifying gaps between policy and process, developing recommendations to remediate control weaknesses and be responsible for developing and maintaining IT control metrics related to compliance activities.   Worked with the IT management team to evaluate controls. Performed assessments, monitored regulations, and worked with auditors to ensure company compliance.   Have in-depth experience in using COBIT, COSO, PCI DSS, OMB Circular A-123, FISCAM and FISMA frameworks in performing the audit.   Performed Audits of application security involving the Company's ERP systems. (SAP, People Soft, Oracle Financial, Deltek Cost Point, People soft) and execute audit strategy.   Performed SAS 70 (SSAE18) reviews for large clients in the Manufacturing, Energy, Healthcare and Financial industry.   Evaluated effectiveness of control activities in order to provide reasonable assurance regarding client's achievement of their business objectives including, accounts payable, accounts receivable and cash disbursements Education BSc. in Business Administration in Business Administration University of NGR Skills audit (5 years), Enterprise Resource Planning (5 years), Oracle (5 years), SAP (5 years), SARBANES OXLEY (5 years) Additional Information SKILL HIGHLIGHTS Highly-accomplished IT Analyst / Auditor with unique background in Information Assurance, Authentication and Authorization, Audit, Risk Assessments, In-depth knowledge of Sarbanes-Oxley Act (SOX), HIPAA, PCI DSS, FISCAM, FISMA, IT General Controls (ITGC), SAS70/SSAE 18 attestation, ERP security assessments (SAP,

PeopleSoft, and Oracle Financials), and NIST 800-53. Proven track record assessing system/network availability, security, and data integrity to identify, manage, and reduce vulnerabilities and ensure general compliance. TECHNICAL / COMPUTER SKILLS Microsoft Word, Excel, SharePoint, SAP, Oracle Financials, IDEA, ACL, NESSUS and Team Mate, Audit Management System, Audit Command Language (ACL), MS Visio, Lotus Notes, ACF2, RACF.

Name: Catherine Gordon

Email: tina33@example.org

Phone: (736)773-8823x12821