Security Risk Analyst (Contract) Security Risk Analyst (Contract) Security Risk Analyst (Contract) I am looking for an IT Security Analyst opportunity in an organization that concentrates on Risk Assessments, Certification and Accreditation (C&A), HIPPA Compliance Assessments, Internal Control Audit engagements, and Information Assurance. I have 3 years of experience in C&A and Risk Assessment of General Support Systems (GSS), Major Applications and Information Security System. Excellent oral, communication, and inter-personal skills.   Areas IT Risk Assessments, Certification and Accreditation (C&A), 3rd party/Vendor Security Control Assessment and IT Auditing. HIPAA, SOX, GLBA, ISO and FISMA. Physical Security, General Computer Controls, Application control, Testing, Compliance Testing, Change Management, Configuration Management, Security Maintenance, Contingency Planning; Policies and Procedures, Implementation, Incident Response, Media Protection, NIST 800-53, NIST 800-53A, NIST 800-30, NIST 800-37, NIST 800-34, NIST 800-18. Work Experience Security Risk Analyst (Contract) Acentia LLC December 2017 to November 2018   Supported in conducting NIST SP 800 to prepare System Self-Assessment and worked with senior leaders to develop and revise detailed contingency plans.

 Performed security assessments, developed and updated Certification and Accreditation (C&A) packages and Authority to Operate (ATO) documentation for systems.   Evaluated the adequacy of internal controls and compliance with company policies and procedures by conducting interviews with all levels of personnel, examining transactions, documents, records, reports, observing procedures.   Conducted IT controls risk assessments that included reviewing organizational policies, standards, procedures and guidelines   Worked with the ISSO and assisted on investigative matters, related to information security, prepare scheduled FISMA reports, Conduct PO&AM reviews, oversight and reporting and Conduct Privacy Impact Assessments.   Provided accurate and precise reporting to the team and senior management   Coordinated data collection, analysis and reporting for IT Security Data Calls and Incident reports.   Conducted walkthroughs, formulated test plans, documented gaps, test results, and exceptions; and developed remediation plans for each area of testing   Conducted reviews on Information Systems security documents for all hosted systems quarterly basis for Plan of Action & Milestones (POA&Ms) and Security Control Test &

Evaluation (SCT&E). Collaborate with IT on Disaster Recovery and Business Continuity Planning; Supported other third-party risk remediation projects as required and needed IT Security Analyst (Contract) Enlightened Inc March 2016 to December 2017 Developed a security baseline controls and test plan that was used to assess implemented security controls. Conducted a security control assessment to assess the adequacy of management, operational, and technical security controls implemented. Assisted in the development of an Information Security Continuous Monitoring Strategy (Ensure continued effectiveness of all security controls), vulnerabilities, and threats to support organizational risk management decisions. Developed a system security plan (SSP) to provide an overview of federal information system security requirements (FISMA) and describe the controls in place. Conduct a Business Impact Analyst (BIA) to identify high risk area where audit effort will be allocated to. Conducted meetings with the IT client team to gather evidence, developed test plans, testing procedures and documented test results and exceptions. Performed IT operating effectiveness tests in the areas of security, operations, change management, and email authentication. Developed audit plan and performed the General Computer Controls testing, identified gaps, developed remediation plans, and presented results to the IT Management team. Conduct IT general controls risk assessments as well as risk auditing with frameworks like HIPAA, PCI. Developed security control test plans and conducted detailed security assessments of information systems that evaluate compliance of administrative, physical, technical, organizational and polices safeguards to maintain HIPAA compliance base on NIST SP 800-66 Rev1 and security controls (NIST SP 800-53). Routine development of HIPAA compliance reports, documenting auditing findings and corrective actions. Trained and supervised staff on HIPAA requirements related to information technology. Assisted in the development of key security standards and guidelines by performing security assessment using frameworks like HIPAA, PCI DSS, ISO 27001 and SOX to help gain compliance. Collaborated on periodic vulnerability review engagements. Information Assurance Specialist Royal Bank of Scotland July 2015 to March 2016 Perform third party Risk Assessment the assess the effectiveness of vendor's control against ISO 27001, HIPAA, HITECH using GRC tools Developed the audit plan and performed the General Computer Controls

testing of Information Security, Business Continuity Planning, and Relationship with Outsourced Vendors.   Identified gaps, developed remediation plans, and presented results to the IT Management team.   Conducted the IT risk assessment and documented the control. NIST 800-37 Certification and Accreditation (C&A) methodologies.   Developed test plans, testing procedures and documented test results and exceptions.   Performed security assessment on cloud hosting applications   Participated in the SOX/FISMA testing and HIPAA, PCI Security Assessments. Conducted walkthroughs, formulated test plans, documented gaps, test results, and exceptions. Developed remediation plans for each area of testing.   Performed IT operating effectiveness tests in the areas of security, operations, and change management Education Bachelor of Science in Public Health in Public Health The Ohio State University

Name: Dustin Hall

Email: jeffrey15@example.org

Phone: +1-752-350-0981x96942