ISO27001 Lead Implementer ISO27001 Lead Implementer IT Security Risk Analyst Washington, DC

Seeking a Third Party Vendor Risk Due Diligence Analyst, IT Security Auditor, or Cybersecurity Analyst position in a growing organization.   CONTROLS & FRAMEWORKS SOC 2 (Type I and Type II), ISO 27001, ISO 27002, ISO 19011:2018, SIG Questionnaire, FISMA, Confidentiality, Integrity, Availability, NIST 800-53, NIST 800-30, NIST 800-37, NIST 800-34, NIST 800-18, NIST RMF framework, PCI DSS and HIPAA.   SOFTWARE AND PLATFORM RSA Archer, SAP Ariba, BitSight, Hiperos, Security Scorecard, Windows, Microsoft Office, Outlook, Power Point, Visio, Tableau. Authorized to work in the US for any employer Work Experience ISO27001 Lead Implementer World Wide Industrial & Systems Engineers (WWISE) - Centurion, Gauteng February 2019 to May 2019   Review ISO27001:2013 and ISO 27002:2013 standards with client to identify potential gaps in required documentation and processes.   Assist with creation of Asset register and conduct a test for its relevance.   Assist in document gathering and evidence collection for audit purposes.   Document security gaps identified as findings that require remediation and/continuous monitoring.   Control documents for easy tracking and accountability. Create standard templates for recording data.   Conduct Risk Assessment and Business Impact Analysis to identify risks that need to be remediated or continuously   monitored. Conduct mock audits for various departments. Cybersecurity Analyst T-Mobile, Bellevue Washington - Bellevue, WA October 2017 to October 2018   Analyze complex enterprise environments from an information security perspective across various industries and identified areas of concern for possible IT audit.   Conduct third-party cybersecurity risk assessments, applying established criteria; Information gathering, questionnaire administration, receive vendor response, risk assessment, reporting and monitoring - using RSA Archer, BitSight and SAP Ariba.   Support assessment team with quality assurance reviews over work product and reporting.   Collaborate with internal partners and third parties to mitigate and otherwise resolve third-party cyber risks.   Consistently deliver on commitments, deadlines and objectives while remaining in scope and leveraging appropriate tools, methods, frameworks and professional standards.   Demonstrate consistent credibility with business partners and leadership while recommending initiatives, identifying gaps and potential issues.   Work independently while

representing the services of the department with the highest level of professionalism. Appropriately influence business decisions, and the professional judgment for selecting the appropriate methods and techniques to do so.   Update procedure documentation to incorporate process changes. Senior IT Risk Auditor Fifth Third Bank - Cincinnati, OH June 2017 to September 2017   Perform third party risk assessments and Vendor due diligence using Hiperos Third Party Management (3PM) tool.   Monitor 3rd party operational risk trends and provide analysis of data and other operational risk metrics using Security Scorecard.   Track exceptions to IT policies and procedures and follow up with management approval for implementation.   Use GRC tool, Archer, to conduct application assessment and track issues identified during the assessment with supporting mitigations measures.   Perform IT & Risk Security Risk & Control Assessments for new products/initiatives   Review services provided by vendor and define scope of assessment. Review assessments performed by 3rd party and provide feedback. Define appropriate risk levels and corrective actions for issues identified.   Report on assessment outcomes, risk level and associated recommendations. Present issues to 3rd parties and obtain corrective action plans. Input corrective action plans into system. Follow up on corrective action plans and review evidence for closure. Provide metrics on a regular basis (KPI / KRI).   Periodically reach out to vendors hosting our data regarding current threats to ensure they are taking necessary steps to reduce exposure as part of ongoing monitoring. Compliance Analyst SmartThink LLC - Greenbelt, MD November 2016 to May 2017   Participated in meetings to discuss system boundaries for new or updated systems to help determine information   types for categorization purposes. Determined the classification of information systems to aid in selecting appropriate controls for protecting the system.   Responsible for conducting structured security certification and accreditation (C&A) activities utilizing the Risk   Management Framework and in compliance with the Federal Information Security Modernization Act (FISMA) requirements.   Report IT security incidents in accordance with established procedures.   Assess adequacy and efficiency of security controls by updating Security Control Assessment Plan (SCAP), Security Test & Evaluation (ST&E) Report and Security Assessment Report (SAR).   Plan, develop, implement, and maintain an Incident

Response and Audit Program for events of interest and address Plan of Action and Milestones (POA&Ms) in continuous monitoring with various point of contact.   Coordinated with system owners and ISSOs across the organization to ensure timely compliance. Credit Card Control Security Analyst First Data - Hagerstown, MD August 2016 to October 2016   Documented potential and actual credit card fraud for analyses.   Processed chargebacks for card transactions that failed to close due network communication discrepancies.   Conducted Business Impact Analysis (BIA) to analyze mission-critical business functions, and identify and quantify the impact of those functions if these were interrupted.   Updated the information systems security documentation (e.g., System Security Plan, Contingency Plan, Contingency Plan Test, Business Impact Analysis, Privacy Threshold Analysis, Privacy Impact Assessment, and System of Records Notice) in accordance with PCI-DSS requirement. Governance Risk & Compliance Analyst Generali Global - Bethesda, MD January 2014 to August 2016   Determined the scope for system audit. Usually started with a kick off meeting with key officials and the audit committee.   Created a test plan to determine controls to be tested as well as methods of testing. Effectively participated in testing of the IT General Controls.

    Conducted audit within specific timeframe utilizing subject matter expects and other system owners Supported requirements gathering and design efforts of critical projects as needed. Collected evidence from various point of contacts to update audit finding report for HIPAA compliance.   Tested for effectiveness and adequacy of controls by analyzing test plan against evidence collected via examination, interview and testing.   Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with company policy. Risk Analyst Generali Global - Bethesda, MD November 2011 to December 2013   Managed, resolved, and closed service tickets regarding queries and customer complaints.   Subject matter expect for benefits and claims management, Coordination of benefits using S.A.X. and C.H.E.S.S. software.   Adjudicated claims according to policy conditions while complying with all legal and federal HIPAA regulations. Created detailed Use Case Scenarios and diagrams to support new System Development. Collaborated with patients and healthcare providers to assist with issues related to payments,

reimbursements, payment denials and appeals. Performed and conducted research on claims inquiries. Documented clearly and concisely claims adjudication decisions in Claim Notes systems. Created Reports to provide snapshots, targets and metrics of claims systems. Practical experience in SAX, CHESS, ICD9, ICD10, HCFA, UB payment and billing. Assisted in training of new employees and worked on multiple special projects. Client Relations Officer Enterprise Insurance - Accra August 2008 to February 2010 Underwrote various non-life policies for individual and cooperate clients taking into consideration inherent risk and current industry standards Managed claim lifecycle from beginning to completion in a timely manner. Coordinated with brokers to manage accounts of existing clients and promote the environment for onboarding potential new clients. Education Master of Finance University of Maryland - College Park, MD December 2016 Master's in Master of Business Administration (MBA) University of Maryland-College Park - College Park, MD December 2016 Bachelor's in Business Administration University of Ghana - Accra May 2007 Skills Negotiation (7 years), ISO (3 years), FISMA (4 years), Risk Management (4 years), Risk Assessment (5 years), Archer (4 years) Certifications/Licenses ISO27001 March 2019 to Present Lead Implementer CSSBB August 2017 to Present Certified Six Sigma Black Belt Additional Information I have over 7 years' experience analyzing and mitigating risks for various entities. My expertise include Assessing Third Party Vendor Risk, NIST Risk Management Framework (RMF), Information Assurance, System Monitoring, Regulatory Compliance and Loss Mitigation. My knowledge of industry standards and ability to meet milestone deadlines make me a valuable addition to any organization focused on staying on top of information security matters.

Name: Kevin Santana

Email: robertnorris@example.net

Phone: +1-313-301-4908x86739