Information Security Risk Analyst - GLBA Compliance Lead Information Security Risk Analyst - GLBA Compliance Lead Information Security Risk Analyst - GLBA Compliance Lead - MUFG Union Bank Tempe, AZ Accomplished IT Security professional with experience in Cyber Risk, Risk, Governance, IT Reviews, Project Management, Access Management, Access Controls, Segregation of Duties(SoD). Experienced in planning, designing, developing and deploying risk assessment methods, and testing strategies for enterprise-level applications. Familiar in all stages of audit including planning, study, evaluation and testing controls, reporting findings, and follow up audit. Ability to understand, and clearly articulate complex technology risks or control deficiencies to technical and non-technical business representatives, and translate into business risks. Be able to recommend security solutions and remediation. Work Experience Information Security Risk Analyst - GLBA Compliance Lead MUFG Union Bank Arizona February 2018 to Present Executing Cyber Security Risk Assessments for regulatory compliance (GLBA, FFIEC, SoX, HIPPA etc.), and critical (payment, settlement, trading, etc.) systems for Americas. Evaluate the adequacy of internal controls and policies, Access controls and Access restrictions, such as controls to authenticate and permit access to customer information systems to authorized persons Leveraging industry standards and input into the Bank's cyber risk management process. Building relationships with key stakeholders by setting expectations and establishing and maintaining communication throughout assessments for their target areas to maximize stakeholders satisfaction Assessing IT security policies, procedures, and controls of our clients' business applications, networks, operating systems, and other components of their technology infrastructure Managing multiple projects and tasks simultaneously, and prioritize risk assessment demands and complete within defined time frames. Conducting risk assessments against corporate technology and security standards Identifying and communicating key control deficiencies to business units Assisting stakeholders with recommendations to address key control deficiencies Evaluating management responses to ensure remediation tasks adequately address identified gaps Performing duties and responsibilities specific to department functions and activities Demonstrated experience in the area of risk and controls across various IT platforms including web, Cloud, applications, database, operating systems, infrastructure, and network security. Implemented policies, procedures, and technologies that ensured Linux system security through secure system access, monitoring, control, and routine security evaluations. Worked with RSA Archer platform. Knowledge of relevant financial industry regulations and standards, with an emphasis on Cyber Security and Privacy requirements surrounding GLBA, SOX, FFIEC, ISO27001, and NIST. Train and support of IT Risk Assessors professionals at offshore on how to do the Gramm-Leach-Bliley (GLBA) risk assessment. Translate the control testing process into Standard operating procedures (SOP's) which includes how the risk assessment should be performed. Perform, and Plan managerial functions related to the IT/IS risk staff (mentoring, training & development, performance appraisals, recruiting qualified team members). InfoSec Risk Analyst WebMD New York April 2017 to January 2018 Control assessments of SoX 404 controls and HIPPA compliance Ensure that risk management controls are implemented and operated correctly on all non-compliant applications in the environment, and work towards remediating them. Ensure stability of IT Production Environment by implementing and managing of application redundant access controls reducing the risk, that only authorized resources are able to obtain access. Identify the risk of unauthorized access from both internal and external networks and work towards minimizing and mitigating the risk. Monitor the inbound and outbound traffics, and remediate them from any risk Improving visibility to trust relationship, which determines who has the privileges on a particular application and its data security regulations Liaise with application owners by resolving the vulnerability issues against the application code (like Code Comparing and Source Code Review). Cooperate and Liaise with regulators by providing required validation reports and compliance reports to close the compliance issues against application(s) by Auditing/validating the application. Monitor and mitigate Day-to-Day security issues meeting the compliance requirements. Manage SIEM user accounts (create, delete, modify, etc.). Create client-specific Watch Lists if necessary Attend vendor-specific meetings and conferences for business and professional development Perform SIEM product support and implementation Database Remediation and Regulatory Coordinator ING Bank New Jersey June 2016 to March 2017 IT Security Compliance, Access Management (IAM) June 2016 to Mar. 2017

Worked on controls assessment and remediation of consumer compliance (GLBA: Safeguard Rule, and Pretexting)   Experience on Complete life cycle of Audit Security methodologies (Planning, Assessment, Mitigation/Remediation, Monitoring, Governance, Risk Acceptance, Communication, Coordination and reporting)   Designed and defined Audit plans, Process, Procedures, test plans and remediation plans according to the industry standard ISO/IEC 27001.   Auditing and filing the Audit reports by Remediated and mitigated the risk on Regulatory in scope applications (Like Trading, Banking, Brokerage, Investment Banking, Internal, External, Financial Transaction and etc)   Managing the remediation with required changes on the individual applications to meet the regulatory requirements eliminating the redundant risk on the production systems   Experienced with IA Provisioning lifecycle, Access Control (RBAC), Access Management (IAM), ACL, Account Security, Database Remediation and Regulatory Coordinator   Audit and identify the risk on privileged accounts towards mitigate the risk.   Assess security related production controls in lines with regulatory standards supporting IT and business processes and finding potential gaps and communicate the risks to key stakeholders.   Auditing the applications and its infrastructure, communicate the findings and gaps to Stakeholders and remediate/mitigate the risk. IT Security Consultant Deutsche Bank New Jersey June 2015 to May 2016   Assess IA Provisioning life cycle, Technical and Application IAM reviews.   Improving visibility to trust relationship, determines who has the privileges to an account and data security regulations.   Perform testing to ensure IT controls of the environment are secure and meet the required SOX regulatory standards.   Work with data owners, leadership teams to Perform data privacy reviews.   Performed reviews to support external audits of SOX.   Assess security related production controls aligned with regulatory standards supporting IT and business processes and finding potential gaps and communicate the risks to key stakeholders.   Access Control, Access Management, Account Security, and work towards mapping them across the bank's environment   Liaise the SOX regulators by providing required validation reports and compliance reports to close the compliance issues against application(s) by Auditing/validating the application. Production Controls & Security Analyst GVS Security Services India July 2012 to November 2014   Liaised functional requirements between business users, development team, DBA, internal stakeholders and vendors. Worked as an application lead for four major telecom applications and interfacing with forty other applications that deal with financial transactions and day to day business applications. Implemented policies, procedures, and technologies that ensured Linux system security through secure system access, monitoring, control, and routine security evaluations. Worked with auditing teams to implement the compliance requirements for FCC (Federal Communications Commission) by identifying the non-compliant items on the application functionality. Established standards, policies and procedures for all aspects of UNIX-based applications on day-to-day issues and activities for multiple applications. Gathered necessary requirements from business and end users and notify development teams. Contact vishveshwarp@outlook.com +1 347-903-1266 www.linkedin.com/in/vish-reddy- 335446189 Education Masters in Computers Science Harrisburg University January 2015 to June 2016 Bachelor's in Computers Science Osmania University September 2008 to July 2012 Skills Ffiec, Glba, Nist, Sox, Hippa, Unix, Oracle, Pl/sql, Sql, Frameworks, Risk assessment, Sarbanes-oxley, Governance, access, training, testing, Security, Active Directory Links http://www.linkedin.com/in/vish-reddy-335446189 https://resume.creddle.io Additional Information Skills DATABASES Oracle SQL PL/SQL OPERATING SYSTEMS UNIX GUIDE LINES(S) & ACTS FFIEC Governance, Risk Assessment, and Compliance (GRC) REGULATION'S: Sarbanes-Oxley (SOX 404) GLBA (i.e. Safeguarding, ID-Theft Red Flag and pretexting) HIPPA GDPR FRAMEWORKS: NIST CSF OCC GLBA FFICE

Name: Levi Palmer

Email: kevin42@example.com

Phone: +1-854-991-8210x337