Compliance Analyst Compliance Analyst Compliance Analyst - Information Security and Risk Atlanta, GA Authorized to work in the US for any employer Work Experience Compliance Analyst Information Security and Risk - Atlanta, GA May 2015 to Present Assisting in the company's corporate initiatives to process daily, monthly, yearly security related requests across various systems.This includes adding and removing user access to systems and documenting all request within their ticketing system Demonstrating foresight in recognizing potential security issues and work with the company's internal partners to develop ways to improve processes. Monitor system access, this would include the generation of ad hoc, monthly and yearly data-entitlement reports.Act as a focal point to responding to security questions. CAMD(Change, Access, Manage & Delete) of a repository of data access rights across all HR-related data systems. Liaising with our technical partners to ensure that technical measures are implemented to conform to HR information security requirements and access rights. Monitoring and reporting on trends of information security and data access issues and make recommendations for corrective actions.Use change control mechanisms to manage changes to our HR entitlement systems. Organizing work and perform duties based on agreed-to schedules.Participate in ad-hoc request.Interfaces with customers(Employees) to assist with information for security requests. Implementing security to include user profiles, roles, page permissions, object security and query security for all areas of PeopleSoft HRMS and Taleo/Fusion products, including HR, Benefits, Payroll, Time and Labor/Kronos, Recruiting, Onboarding, Goals/Performance, Compensation, etc. Maintaining all levels of Department security, including approval process flow, data permissions, Department table and Department tree setup. Maintaining and updating user security profiles for multiple reporting directories (Vista, Pay Center Directory, Controller Check Print Folders, and LBC Directory). Acting as a Subject Matter Expert(SME)for projects and implementations, which may include weekly status meetings, joint application design sessions and testing sessions.Working with other functional and technical resources to ensure that security standards and established processes are adhered to during projects and implementations. Supporting information security audits from an application data perspective and perform risk assessment including risk identification, risk mitigation and

documentation.Resolves security related tickets passed to ISR team within the Service Level Agreement(SLA) and PLA. Providing technical support to employees regarding the resolution of product hardware, software and operating system issues via phone or remote access for all supported applications or products.Responding promptly and professionally. Analyzing employee logon issues to determine if resolution can be found on initial call or if second level support is required. Supports and installs upgrades and assists in all technical problems (i.e.. performance, security, etc.) Effectively troubleshoots, replicates and develops workarounds for client issues.Documents and communicates the results to the client and/or Corporate Development.Maintains appropriate records of client contact through the CRM system.Uses Knowledge Management database to locate solutions to issues.Ensures case notes thoroughly detail the problem/resolution, are comprehensive of the issue and are professional. Providing on-site assistance on issues that could not be resolved via remote tools, ie. deliver service packs, set up reports, install or upgrade software or develop custom solutions for all client server products.

Performance issues related to client infrastructure integration are referred to a peer with specialization in the particular platform or application (Citrix, Lan/Wan, Client Server, etc) Provides complex technical expertise for industry standard database applications, ie MS Access, Oracle, mySQL, MS SQL Server, etc. Assisted in new product pilots and roll outs to other departments and clients. Acts as liaison between Implementation, Client Services, Management and Corporate Support to ensure high impact problems are resolved in a timely and satisfactory manner. Administration of network and computing devices/systems that help enforce security policies, audit controls and in a global environment.Assist in responses to external audits, penetration tests and vulnerability assessments Coordinating maintenance of security-related systems (Anti-Virus, Patching, Intrusion Detection, Logging, Anti-spam, etc.) Daily administration of monitoring tools, including maintenance and upkeep Daily monitoring of enterprise networks and management of alert notifications for suspicious/malicious behavior. Identify security issues and risks, and develop mitigation plans.Implementing technical solutions to support regulations as required coordinating the application of fixes, patches and disaster recovery procedures in the event of a security breach.

Respond in a timely manner to suspected loss or misuse of information technology assets Participating in investigations of suspected information technology security misuse or in compliance reviews as requested by auditors.Participate in and acts as a technical leader in, periodic information systems risk assessments including those associated with the development of new or significantly enhanced business applications Communicating unresolved information technology security exposures, misuse, or noncompliance situations with appropriate management Providing users and management with technical support on matters related to information security such as the criteria to use when selecting information security products Advising Information Technology Security Officer on technologies, practices, and policies that can mitigate security issues.Monitor current and proposed laws, regulations, industry standards, and ethical requirements related to information security and privacy Conducting research on emerging products, services, protocols, and standards.Assist with compliance validation and reporting. Identification of vulnerabilities with the Bank's environment with oversight of associated remediation activities. Information Security Analyst HONKONG AND SHANGAI BANKING CORPORATION - New York, NY March 2014 to April 2015 Worked closely with the global Information Security and Compliance team to implement security standards across the organization. Performed audits of IT systems and evaluate against technical controls and operating procedures. Ensure audit findings and evidence are collected, reviewed, remediated, and presented in a clear and concise manner. Worked to continually refine controls and processes. Documented audit procedures, make recommendations, and follow-up to validate implementations. Identify and evaluate business and technology risks, internal controls which mitigate risks, and related opportunities for internal control improvement. Assisted in the selection and tailoring of approaches, methods, and tools to support service offering. Facilitated use of technology-based tools or methodologies to review, design, and/or implement reviews. Implemented policies and procedures in all concerned business areas and ensure that audit requirements are met in day-to- day operations. Administrated and maintained environment security. Involved with administering security alerts to staff and weekly data backups. Performed hands-on administration, monitoring, and troubleshooting of Local Area network (LAN), resulting in

optimum performance and minimum downtime. Creating and managing Windows NT/2003 user accounts and profiling them. Application groups, and shared directories access across 2 different domains in different locations of HSBC users. Created of Lotus notes accounts and trouble shooting of LN(Lotus notes) Issues. Took ownership and resolve IPT issues, consult , coordinate with peer group across regions to resolve more complex problems Maintained servers for network, including backup and upgrades Managed users/objects in Active Directory, set up new objects/OU's/containers and on Taleo records mantainance. Created, maintained and troubleshooted group policy. Completion of Ad-hoc requests with in the time and providing good support to the client(User).Administer Microsoft Windows Servers (Active Directory), Microsoft Workstations, and network security devices for world wide users of HSBC. Provide access provisioning on Mainframes platform & other critical security applications for internal customers/users(HSBC). Resolve tickets and requests pertaining to access control s for our internal customers with in the agreed SLA(Service Level Agreement) and PLA(Process Level Agreement).Resolve a high percentage of tickets by proper usage of inbuilt procedures in the knowledge base/ any other knowledge tool that is provided by the Business. Analyzing functional requirements and developing technical solutions using PeopleSoft program. Supporting employees with information security questions by administrating their logon ID's with Given access permissions.Proactively protect the integrity, confidentiality, and availability of information technology resources. IT Security Analyst VERIZON - Tampa, FL January 2010 to March 2014 Responsible for supporting the initiatives of the corporate information security program and coordinating with various IT Delivery and Operations teams. Significant, hands-on, tactical approach to the operational aspects of information security. Monitoring and response for alerts from key security technologies and other internal sources. Researching emerging threats, evaluating likelihood of occurrence, and controls to mitigate them Automating manual processes, assisting with creation and maintenance of Runbooks / Service Catalogs, etc. Incident managements(CAMD-Change access manage and deletion) of Accounts and trouble shooting the issues with"REMEDY" ticketing tool Experience of network analysis tools, scripting languages,

software vulnerabilities, exploits and malware Experience of network traffic analysis for identifying any developing patterns Ability to assume leadership role on ad-hoc basis for managing Level 1 Analysts Experience of working in a high volume and result-oriented operational environment Ability to read and understand system data including security event logs, system logs, application logs, and device logs, etc. Possess solid understanding of enterprise grade technologies including operating systems, databases and web applications and Applicable monitoring tools (e.g. SIEM, DLP, Internet filtering/blocking, IDS/IPS, firewalls, Anti-Virus, encryption technologies) Demonstrated network traffic analysis capabilities for identifying any emerging patterns, network infrastructure knowledge, Security configuration knowledge. Education Bachelors of Engineering in Computer Science and Information Technology Engineering Jawahar lal Nehru Technical university - Hyderabad, ANDHRA PRADESH, IN Skills INFORMATION SECURITY (7 years), SECURITY (7 years), MAINTENANCE (6 years), DATABASES (4 years), AUDITS (3 years) Certifications/Licenses Cisco Certified Network Associate (CCNA) Additional Information TECHNICAL SUMMARY: Compilation of information security reports including data leakage, vulnerability management, phishing incident trends, user access. Documentation collection, organization and tracking for IT-related audits and examinations conducted by both internal and external parties. Supporting employee security awareness activities, communications and exercises. Coordinate social engineering exercises and compile results.Following IT policy and procedure maintenance and updates. Participating in business continuity planning efforts and exercises, and compile exercise reports. Maintain and update corporate emergency notification application. Good understanding of TCP/IP protocolos,Routing protocols like BGP,EGRP to resolve the Connectivity issues. Providing technical support to all levels of Service Support Specialists regarding the resolution of product and client issues. Mentoring and trains newly hired associates to ensure successful integration into the role. Identifying training needs for the department and assists with training development programs. Provides feedback to management. Acting as a team leader in the absence of the manager by prioritizing critical issues, providing direction and ensuring appropriate client support is delivered in a timely and effective manner.

Staying current with emerging technology and trends in order to provide technical support for product rollouts and/or existing offerings.Proficient on networks, operating systems, hardware, software, databases, browsers and related products. Assisting in developing internal documentation to support new features and procedures for product enhancements.Performing other related duties as assigned. Assisting with information security investigations and e-discovery processes as needed. Performing and maintains compliance efforts with various laws and industry regulations including Payment Card Industry Data Security Standards (PCI-DSS), Sarbanes-Oxley (SOX) and HIPAA.

Name: Renee Phillips

Email: leslie89@example.org

Phone: (755)886-6741x29581