IT Systems Analyst - Security IT Systems Analyst - Security IT Systems Analyst - Security - Experian Irvine, CA Established and seasoned Information Security Analyst with over 8 years of experience in the Healthcare and finance Industry working in Information Security. Hands on in specialization in Compliance Standards, application security, data security, system engineering and administration. Experienced in Credit Monitoring system, Billing Systems, HIPAA 4010-5010 conversion, ANSI EDI X12 transactions sets -834, 835, 837 and 270, PCI. Adept in creating Wireframes and UI Mockups. Familiarity in data analytics with a strong ability to write efficient SQL queries and extract information. Excellent interpersonal and soft skills, including written and oral communication skills that are pivotal in carrying out responsibilities efficiently. SPECIFIC SUMMARY: Over 8 years of Business Analysis, Infrastructure and Security experience with specialization in Compliance Standards, application security, data security, system engineering and administration. Proficient in conducting Brainstorming sessions to gather high level requirements, conducting JAD sessions, and preparing JAD documents Experience in developing Business Requirement Documents, Functional Requirement Documents, Systems Specifications, and Functional Specification documents Highly experience in conducting GAP analysis determining AS-IS and TO-BE processes Proficient in creating user stories, estimating the size of user stories and prioritizing them Good experience in conducting various SCRUM ceremonies such as Sprint Planning meeting, Daily Scrum, Sprint Review Meeting, Retrospective meeting and product backlog grooming. Experience as a SME and privacy/ security analyst with applicable knowledge of regulatory compliance procedures related to SOC and PCI. Experience in building KPI reports to businessusingSQL Server 2012. Extensive knowledge on the industry standards HIPPA, PCI, SOC. Hands-on experience with vulnerability assessment tools and techniques, security event management tools, information security monitoring, enforcement, design, authentication and multi-factor access control systems and malicious code control. Work directly with production support teams regarding Vulnerability Remediation efforts for OS, Data Base & Middleware systems and Applications. Hands-on experience with SIEM configuration, creating & fine-tuning rules. Proficient in analyzing different security threats to organizations by identifying the indicators that a

security incident is underway and investigation methods use to collect evidence for prevention and prosecution. Experience in using RSA Archer eGRC application platform to build Reports and support API's. Active participant in coordinating with different teams such as Network Engineering, Database team and application teams to resolve the issues and provide Customer Satisfaction. Certified professional by Qualys enterprise on Web Application Scanning, Vulnerability Management, PCI Compliance, Policy Compliance, Advanced Vulnerability Management Experience with IT System Development Lifecycle (SDLC) Management ensuring that security requirements are planned, implemented, operating and updated appropriately. Detail-oriented and dynamic self-starter, effective leader and team player with a strong interest in learning and innovation with the ability to make clear and convincing oral presentations to individuals or groups. Work Experience IT Systems Analyst - Security Experian - Irvine, CA June 2015 to Present The scope of the "Secure First" project initiative (Information Security) was to implement security protocol for all the Intranet and Internet applications. Worked closely with the vendors, Application Security teams, Application Development teams and SMEs. This initiative includes all the business lines (Financial, HealthCare and Credit Services) Supporting Integration and Business teams on solutions and deployments with access controls and security standards. Worked with security SME, software and hardware technology architects concerning infrastructure operations, access compliance and security policies. Performed risk assessment as per industry security standards. Worked with change management team in implementing problem and change management process as per industry standards. Proactively identified opportunities to improve various processes, including increasing operational efficiency, providing increased automated monitoring, capacity planning and governance controls. Adhered to existing processes/standards including the System Development Life Cycle (SDLC) and project management methodologies, business technology architecture, risk and production capacity guidelines and escalate issues as required Experienced with providing quarterly reports from Remedy by filtering data, and running queries using SQL. Worked with network team in implementing firewalls, network sniffers and email scanning systems as per company security standards. Implemented quarterly security and vulnerability scanning

systems and generated security reports. Worked closely with server team in remediating the vulnerabilities. Implemented patching policies based on PCI compliance and change control process for patching policies. Identified computer security incidents by characterizing the nature and severity of incidents among the Firm's community both internally and externally. Conducted planning activities and prepared associated documentation in support of cyberspace operations. Provided immediate diagnostic and corrective actions in order to maintain the company's Security Infrastructure. Develop success indicators and KPIs Apply various methods to solicit program feedback including questionnaires, evaluation forms, interviews, focus groups, formal status reports, selective interviews etc. Investigate and implement ongoing program improvement strategies Created configuration Tables, Stored Procedure, User Defined Function in SQL Server Management Studio to support the whole SSIS process workflow. Tested Database activities and Automated Database test cases (SQL) test cases and executed Worked extensively with Business Users and SME's including high level leads in understanding, refining and documenting the User and Business Requirement Specifications in the BRDs. Scheduling the SSIS Package Execution by Using the SQL Server Agent for monthly data loads. Imported and Extracted data from various sources such as flat file, access, SQL server and loaded those data into SQL server to build various reports. Created various Documents such as Source-to-Target Data mapping Document, and Unit Test Cases Document. Automated all the reports extracting process in the new system by using custom store procedures in SQL 2014. Information Security Analyst Disney Imagineering - Glendale, CA July 2014 to May 2015 Scope of the project was to take the Security initiatives in the financial portfolio of Walt Disney Parks and Resorts. Worked closely with the Compliance, Application security teams to implement the SOC compliance standards. To ensure projects and existing systems have the appropriate level of security, privacy, and compliance controls. Periodic assessment of systems and coordinate security exception process (when needed) and will work with the Parks & Resorts Compliance Team to support compliance requirements and investigations. Conducted as-is analysis and GAP analysis for the current state and to-be state of the system Coordinate internal and external audit work over IT operations and processes; liaise with IT teams in

gathering documents and testing related IT controls during audit reviews Work closely with functional senior leaders to ensure threat intelligence analysis and products are mapped to prioritized corporate assets and risks. Manage the policy, standards and procedures framework for Information Security & IT Risk/Compliance. Developed security incident escalation processes and solutions for the SOC. Researched and recommended threat mitigation / incident response techniques. Escalated incidents directly to Account Security Leads and Security Incident Response teams. Applied QRadar SIEM tuning methods for emerging threat patterns and the mitigation of false positive security alerts. Conducted QRadar SIEM correlation review meetings. Worked directly with Threat Intelligence experts on discovery and analysis of newly emerging attacks. Gathered requirements after conducting Discovery workshops with the purpose of defining the business and system requirements. Created UML Diagrams including Use Cases Diagrams, Sequence Diagrams, Activity Diagrams, Data Flow Diagrams (DFDs) and Web Page Mock Ups using Rational Rose and MS Visio. Performed AS-IS and TO-BE analysis and documented as GAP Analysis. Reviewed legacy version of Business Requirements Document, Business Regulations and Design Specifications in detail. Conducted highly interactive JAD sessions with product owner, project stakeholders, development and QA team, as well as SME's in identifying and resolving issues and setting project direction. Defined quality attributes, metrics, external interfaces, constraints, security and other non-functional requirements. Utilized communication, problem solving, analytical and innovative thinking skills in understanding ongoing challenges to suggest enhancements and optimize effectiveness. Facilitated User Acceptance Testing to ensure the system is sufficient and ready for business usage. Documented Test Plans, Test Scripts, Log Defects, and Requirements and uploaded to HP Quality Center for future follow up and bug fixing purposes. IT Systems Analyst - Security Experian - Denver, CO September 2013 to May 2014 Scope of the project was to take the Security initiatives in the Consumer Services Business line of Experian.I was part of the Compliance, Application security teams to implement the SOC compliance standards. Developed an Enterprise wide compliance program integrating PCI requirements, SOC controls Information Security policies into a single, coordinated and unified

program satisfying regulatory, legal and Information Security policies and requirements. Developed and documented IT processes and procedures specifically to identify PCI and SOC controls and gaps. Maintained and managed the Information Security policy. Successfully developing several information security policies including an Acceptable Use policy for employees and contractors, Mobile Device and Key Management policies. Conducted JAD sessions with management, SME, vendors, users and other stakeholders for open and pending issues Implemented a policy change management process, tracking policy changes, management approvals and versions. Successfully completed full Risk Assessments on Change Management, Access Management, Logging & Monitoring, Patch Management, Network Security and Configuration Management. Identified and communicated several risk areas that would significantly reduce DKRIN risk footprint. Coordinated with IT management to remediate risks. Successfully completed a series of process improvement assessments for Security Operations, Encryption and Data Storage management processes. Provided recommendations to IT Senior Management that would elevate their overall process maturity rating by one level. Developed and implemented DKRIN Security Awareness program writing over thirty monthly security related articles for DKRIN Corporate Office, Distribution Centers and Stores. Information Security Analyst Sharp Health Plan - San Diego, CA October 2009 to September 2012 The scope of the project was to standardize the reports for all the Business Lineswithin the organization. As part of an enterprise wide initiative, an internal business analytics system was created to transform its reporting process. The resulting report creation, distribution and research became much more proficient and flexible, saving the company money and staff hours. Primary responsibility is to serve as a project manager to pursue, manage, and execute cyber security projects Conducting assessments of systems and networks, implementing technical controls, and documenting the mitigations related to the security of computer systems and networks in corporate and secured environments Coordinate internal and external audit work over IT operations and processes; liaise with IT teams in gathering documents and testing related IT controls during audit reviews Follow up with IT teams for any non-compliance issues and coordinate plans for remediation/ mitigation of risks and

exposure; review remediation results Provide consultancy in defining the improvement plans and procedures for enforcement and compliance of corporate policies and standards Conducted JAD session with project's stakeholder identifying problems and coming up with the best alternative to resolve issues Created targeted questionnaire for SME to gather requirement Communicate security and compliance issues in an effective and appropriate manner throughout the organization across different regions. Follow up with IT teams for any non-compliance issues and coordinate plans for remediation/ mitigation of risks and exposure; review remediation results Provide consultancy in defining the improvement plans and procedures for enforcement and compliance of corporate policies and standards Work with SCCM and Change management team to ensure effective patch and updates package management. Create various business documents such as technical and functional requirements, information security policies and post mortem documents. Manage patch Management Policy and drive the patching program. Security Awareness Program Procure/create catalog of information security content and deliver training on a regular basis to all staff Structure and develop the strategy and plan to implement security awareness program Conduct needs assessment Develop awareness training material, baseline to NIST Special Pub. 800-16. Monitor compliance of the program to organizational goals and industry standards Develop success indicators and KPIs Apply various methods to solicit program feedback including questionnaires, evaluation forms, interviews, focus groups, formal status reports, selective interviews etc. Investigate and implement ongoing program improvement strategies Systems Analyst - Security Cigna Healthcare - Denver, CO May 2008 to September 2009 The scope of the project involved enhancing the legacy web application for Cigna Healthcare. New process implemented which allows the user to check deductible pay of the contract, create, view and delete claims. The system also equipped guest users with more features such as finding urgent care and providers. Additionally, the GPS feature was enhanced in this update so users could locate their nearest providers. Installation, configuration and administration of Linux Servers; Set up and configuring of Linux servers/workstations for clients. Configuring the NFS servers, setting up servers in network environment and configuring FTP/NTP/NIS servers, clients for various

departments and clients. Experience working with high availability, high performance, multi-data center systems and hybrid cloud environments. Handling the scheduling tasks (cron jobs and task scheduler) for the scripts for various purposes. Raising tickets for change management and make sure change management process are being followed for development. Troubleshoot complex issues ranging from system resources to application stack traces. Extensive knowledge of Linux/Windows based systems including hardware, software and applications. Creating a change requests, work orders and problem tickets using BMC Remedy tool and getting approvals from higher officials. On-call support for 24/7 for troubleshooting production issues. Project Management for various UNIX/Linux/Windows system integration projects. Education Masters in Product Management Texas A &M University Bachelor of Technology in Computer Science & Engineering JNTU Additional Information TECHNICAL EXPERTISE: Operating Systems Microsoft: Windows XP/Vista/7/Server 2003/Server 2008; Linux: CentOS, Red Hat, Ubuntu Server/Desktop, Linux; SDLC Methodologies Waterfall, Agile (Scrum) Business Skills Change Management, Impact Analysis, JAD Sessions, SWOT Analysis, Project Planning Management Tools MS Project, MS SharePoint, Clear Case Hardware Guardium Appliances, QRadar Appliance, Network Interface Cards, Video Cards, Memory, Printers, Computer Peripherals, CCTV Surveillance. IDS/IPS McAfee Intrushield / NSM, McAfee e-Policy Orchestrator (ePO), Source fire, ISS Site Protector. SIEM IBM QRadar, Splunk, ArcSight ESM. Log Analysis Cisco ASA, Palo Alto Networks firewall, UNIX syslog, Juniper, ArcSight, McAfee Intrushield / NSM. Software Qualys Guard, OpenVAS, Guardium, Wireshark, Snort, Norton Antivirus, Avast Antivirus, Malwarebytes, Norton Ghost, HP Quality Center, Active Directory, Microsoft Word/Excel/Access/Visio, IIS, Apache, Service Now. Network Protocols Ethernet, LAN/WAN/MAN, TCP/IP, DNS, DHCP, FTP, TELNET, SMTP, POP3, SSH, UDP, ICMP, IPsec, HTTP/HTTPS. Data Base Oracle DB, Microsoft SQL Server.

Name: Andrea Lyons

Email: alisonmendez@example.com

Phone: 001-957-242-2360x91709