St. Joseph Health, Senior Security Analyst (employee) St. Joseph Health, Senior Security Analyst (employee) St. Joseph Health, Senior Security Analyst (employee) - Information Security Services Dept Stanton, CA 10 years of IT Audit Experience: I have been the IT Audit Manager for 3 Fortune 500 corporations (Countrywide Financial Corporation, Home Savings of America and PacifiCare Health Insurance Company). I hired and trained IT auditors, and developed audit department policy and procedures. I performed annual company-wide IT risk assessments to develop annual IT audit plans that significantly reduced annual external auditor Management Letter IT control findings. I reviewed IT audit work papers, edited audit reports, coordinated annual external financial auditor IT audits and state/federal regulatory IT examinations. 8 years of Information Security and IT Regulatory (GRC) and Privacy Compliance Experience: I have been the Information Security Manager at two Fortune 500 Companies (Hughes Aircraft & PacifiCare Health Systems), which included the following accomplishments: Implementation and administration of Privacy Programs to protect confidential customer data from identity theft; ensuring regulatory compliance with HIPAA, GLBA, and Payment Card Industry (PCI) regulations; IT Department Risk Management, Controls and Regulatory Compliance management; website and network security penetration testing and vulnerability scans. Three years' experience using the RSA - Archer GRC system for performing and tracking outsourced IT vendor risk assessments, Graham-Leach-Bliley and HIPAA compliance assessments/audits. 5 years IT Sarbanes-Oxley (SOX) ERP security and control review experience: I automated SOX control testing by using IBM SharePoint to organize documentation, PWC's Internal Control Workbench and Resource Global's Policy IQ to improve SOX IT General and Application Controls control testing and remediation for twelve corporations in Southern California (2003-2011) using the COSO, COBIT, AICPA and the PCAOB SOX Audit Standards. I significantly reduced the cost of maintaining SOX IT control documentation and testing by automating controls, control testing and reducing the number of key IT controls. I have audited SAP ERP, Oracle Financials, J.D. Edwards and PeopleSoft general ledger systems. I reviewed and documented the security, controls, audit trails, Key SOX IT general ledger controls in a process narrative documentation and then tested the controls for both the ERP system and its supporting

infrastructure. I designed and implemented the built-in application security of an Oracle and a SAP ERP system. I scanned a SAP ERP system with the Protiviti GRC Segregation of Duties (SOD) Tool to identify and remediate risks by implementing roles based access. SAP modules included: Basis, A/P, A/R, Inventory, payroll, userID provisioning, Master Data, shipping/receiving, manufacturing, bill-of-materials and fixed assets. 8 years of IT Risk Management Experience: (Farmers/Zurich Insurance, State Farm Bank, Accenture, Bank of America, and St. Joseph Health) I coordinated a global IT risk assessment of 25 company-owned data centers and 3 outsourced IT vendor data centers for a global insurance company using the UK's International Security Forum (ISF) methodology. I summarized risk results into a management summary report and implemented a monthly status follow-up program to coordinate mitigation action which reduced risk by 70%, significantly reduced costs, reduced "SEV1" outages by 60% and improved IT department service levels (SLAs) to business units. At Providence St. Joseph Health as a Senior Security Analyst I coordinated HIPAA compliance for 100 hospitals for 1100 enterprise-wide and hospital applications. I have extensive experience in outsourced IT vendor relationship management and risk assessments. 4 years experience with Customer Relationship Management (CRM) and Call Center IT systems and business operations: As a contract consultant for Accenture several of my data privacy risk assessments involved reviewing the security and controls of hosted IT and business process outsourced CRM systems for cell phone companies in Italy and Greece, 2 large public utility companies, and the Hilton Hotels Global Front Desk Reservation system. CRM systems are also considered very high risk by Bank of America in Outsourced IT Vendor Assessments as the Call Center personnel have access to non-public personal information (NPI) of customers which we protected with roles based access, encryption, audit trails and also computer-telephone integration (CTI) with the AVAYA and Genesys call center systems. At Providence St. Joseph Health I developed a mobile computing device / smartphones security standard utilizing the MobileIron Mobile Device Management system in hospital doctor, nurse, patient call/messaging systems to ensure confidential patient HIPAA data is secured. Work Experience St. Joseph Health, Senior Security Analyst (employee) Information Security Services Dept August 2015 to Present Application

Security HIPAA Compliance Program: (100 hospitals in western USA) As a Senior Security Analyst in the Information Security Services Dept., I have helped merge the information security departments of the two merged companies Providence and St. Joseph Health. I wrote new policies, procedures and standards to facilitate merging the security operations of the two companies. Then I coordinated the review and approval of these draft policies with the Compliance/Privacy, Legal, Human Resources and IT departments, to minimize impact to operations and help ensure meeting company business objectives. I am responsible for leading the periodic review of key IT security/controls identified in the company's Integrated Control Framework, HIPAA regulation and using the RSA Archer system. I train system owners on the information security assessment process. I advise project managers and system owners on how to remediate security, control or compliance findings. I analyze security assessment results for trends and patterns that indicate vulnerabilities that could be exploited, and then recommend and project manage implementation of new security systems and monitoring. I develop executive management summary status reports using Archer, Excel and PowerPoint to flag high risks that need to be remediated. I have developed security standards and risk assessment processes for cloud computing, Proofpoint Data Loss Prevention (DLP), hospital WIFI and cellular based secure (encrypted) doctor/nurse call systems. This required development of a Bring Your Own Device (BYOD) standard to support security, control and HIPAA regulatory compliance for all kinds of mobile computing devices, primarily smart phones. I developed security and control standards and for outsourced IT vendor management oversight. Project Lead - Risk Monitoring for the Graham Leach Bliley Act (GLBA) Compliance Program TEKSystems Agency - Bloomington, IL February 2014 to August 2015 Corporate Headquarters in Bloomington, Illinois, Project Lead - Risk Monitoring for the Graham Leach Bliley Act (GLBA) Compliance Program: As the Project Lead - Risk Monitoring, I was responsible for coordinating the review of Key Controls identified in the company's Integrated Control Framework as important for GLBA and PCI compliance. I developed a program to create a central database system of record of all assets that store process or transmit customer non-public information, this includes IT systems, business processes, vendor and outsourced IT systems. All assets containing confidential data were

inventoried, classified, risk ranked and prioritized for regular testing and monitoring to ensure they are designed and operating effectively. The process included manual and automated control testing, including IdentityIQ, SailPoint's governance-based Identity and Access Management (IAM) software solution for automating compliance, password management and provisioning activities for applications; Security Information and Event Management (SIEM) for central network and computer device log aggregation, log analysis, compliance reporting, file integrity monitoring, user activity monitoring, object access auditing, event correlation, log forensics, threat and vulnerability scanning, monitoring and management. Security and control weaknesses were tracked in the RSA Archer GRC system and other IT Help Desk "ticketing" systems for status tracking. IT Vendor Assessor client Bank of America - Charlotte, NC November 2012 to November 2013 in the Global Business Continuity and Information Security Department: I performed assessments of the security and controls of Bank of America's largest and highest risk outsourced IT vendors. The emphasis was on data confidentiality, availability and integrity, as well as to reduce the risk of identity theft of Bank of America customer data. In order to ensure compliance with the bank's Global Information Security Standards and IT Service Provider Requirements. Bank of America requires outsourced IT service providers to adhere to the Bank's internal standards. The Bank of America Enterprise Vendor Testing Program tests the service provider's compliance with the standards annually based on risk ranking. Areas of emphasis were: Facilities Management (data center physical security and environmental controls), Human Recourses/Personnel and subcontractors oversight, Network Access Control and operations, IT Security Management, Incident Management, Payment Card Industry (PCI) compliance, Platform administration of servers, network routers, switches and firewalls; databases, websites, patch management and vulnerability/penetration testing, application development and maintenance, business continuity/ IT disaster recovery plans, encryption and website security, and compliance to FDIC and OCC federal banking regulations. Types of IT vendors included: law firms, collection agencies, mortgage loan servicers, mortgage loan modification companies, customer relationship and contact call centers, stock brokerage firms and bankruptcy settlement processing. IT Consultant client Accenture - Chicago, IL October 2011 to

June 2012 in the Accenture Global Information Technology Risk Department: I performed data privacy audits of the largest and highest risk IT Accenture global projects to verify the level of compliance to the Accenture Information Security Standards, terms of the contract, the client's policies and applicable privacy regulations. The focus of the audits was analyzing and testing project documentation and interviewing project personnel to determine the level of compliance risk. A final report was issued that described the findings and the remediation plans, which I was also responsible for tracking and verifying through implementation. Clients included cell phone companies in the European Union, global hotel chain front desk and reservation system, public utilities and several large insurance companies. Risks included liability, identity theft risk and potential negative publicity or regulatory action. IT Consultant Resources Global Professionals - Los Angeles, CA September 2006 to October 2011 I documented SOX IT controls in a process narrative format, evaluated key IT control designs, tested the IT general and application key controls. I recommended key IT control remediation and verified implementation of management action plans and retested the controls, based on the PCAOB, COBIT, COSO and IT Governance Institute guidelines. I performed Information Security, IT Audit, privacy, regulatory compliance and IT risk assessments. I performed IT project risk consulting, on-call IT security incident support, internal and external audit support for the Global IT department for international insurance company. I project managed an accounts payable and procurement business process outsourcing (BPO) project for a large mortgage company. Lead Information Security and Compliance, Information Technology Department Ameriquest & Argent Mortgage - Irvine, CA September 2005 to September 2006 I implemented processes to automate and reduce the cost of regulatory compliance by implementing internal controls to ensure compliance with all State and Federal regulations. I coordinated all internal and external audits of the IT department. I coordinated vulnerability scans of databases, operating systems, Cisco routers/switches, firewalls and I analyzed, risk ranked, prioritized and reported on the status of remediation. I administered the process to obtain the Argent CIO's quarterly and annual SOX Certification report to the Audit Committee of the Board of Directors. I tested SOX "key" IT general and application controls to ensure compliance and control design had

not changed. IT Contractor/Consultant Arose Recruiting - Newport Beach, CA September 2004 to September 2005 During a one year contract for IT Audit and SOX IT Controls project at Pacific Life Insurance, I documented SOX IT controls in the client's standard process narrative format, evaluated the control design and tested the control effectiveness of IT general and application key controls and trained SOX project team members on SOX IT controls design and testing. I recommended remediation and verified implementation of management action plans and retested the controls, based on PCAOB, COBIT, COSO and IT Governance Institute guidelines. Engagement Manager - Information Technology Practice Jefferson Wells International - Irvine, CA November 2003 to September 2004 I marketed, project managed and delivered consulting services for information security and IT audit. I performed Sarbanes-Oxley compliance consulting for the K-Swiss, Sempra Energy and Alliance Imaging corporations. I provided major IT projects implementation analysis for two advanced transportation management projects for the City of Los Angeles Metropolitan Transportation Authority (MTA) with budgets of over two hundred million dollars. Manager Information Security Department, Corporate Information Technology Department PacifiCare Health Systems - Cypress, CA 1999 to 2003 After promotion and transfer to the IT department, I was responsible for regulatory compliance analysis and remediation implementation for HIPAA, Sarbanes-Oxley, Graham-Leach-Bliley and California's SB1386 privacy regulations. As a manager and consultant in the Information Security dept., I also supervised a staff of 10 that performed userID account administration and password resets for over 200 applications and systems. I implemented automated processes to improve efficiency and service levels. I performed cyber-forensic investigations of IT policy violations and served as part of the Computer Incident Response Team (CIRT) for virus and hacker incidents. I implemented an Intranet based self-service password reset system that reduced the number and cost of help desk calls by 40%. I implemented Virtual Private Network (VPN) and CITRIX remote access systems, reducing "1-800" remote PC dial-up charges to provide secure remote access to employee telecommuters. I implemented an email anti-spam system and Internet usage filtering system that significantly reduced costs and improved employee productivity. IT Audit Manager - Corporate Audit Department PacifiCare Health

Systems - Cypress, CA 1997 to 1999 I started up the IT audit department for PacifiCare with 3 IT auditors, developed audit programs, risk analysis and annual EDP audit plans. I performed, supervised and reviewed audits in the following areas: data center security, disaster recovery, production program change control, PeopleSoft, data warehouse security, DEC/VAX, Windows NT and UNIX operating system security audits, dial-up modem security, EDI and FileNet imaging systems. IT Audit Manager - Internal Audit Department Countrywide Financial Corporation - Pasadena, CA 1996 to 1997 I started up the IT Audit Department and supervised a staff of four IT auditors. I designed and tested the security of Countrywide's Internet "Virtual Back Office" loan origination system. I reviewed the physical security and Disaster Recovery Plan for the main data center. I used AS/400 queries to analyze loan asset quality for the Loan Loss Review Committee and to investigate various types of fraud and look for reasons behind suspicious trends in loan foreclosures. I audited and significantly reduced the risks in the wire transfer system and interest rate risk hedging system. I significantly improved the "loan audit" function that was the interface between the loan origination branches and the centralized loan service department, by improving the front-end application edits and quality of loan document files which reduced the cost and time to set up a loan for servicing and sale of mortgage backed securities. IT Audit Manager - Internal Audit Department Home Savings of America - Irwindale, CA 1991 to 1996 I supervised a staff of 15 IT auditors. I provided support for external CPA audits, state and federal regulatory bank examinations of Home Savings. I did an annual risk assessment and then planned, scheduled, budgeted, performed or reviewed IT audits on the corporate data center, telecommunications network, databases, applications, websites, ATM and wire transfer systems. My IT audit work helped the company receive "excellent" regulatory examination ratings, resulting in lower capital requirements. I coordinated IT application audits with the related financial and operational audits to provide one "integrated audit" report. I recruited hired and trained IT auditors, trained CPA auditors that wanted to become IT auditors and several of my IT audit staff were promoted into key IT department positions. I was a member of several high level IT strategic planning committees. My IT audit staff played a significant role in the successful implementation of a $100 million dollar integrated loan

origination and loan service system and the implementation of imaging technology in the item processing department. Manager, Computer Assurance Services Department Deloitte & Touche - Irvine, CA 1989 to 1991 I was responsible for performing, project managing and marketing consulting services for: information security, business continuity planning, contract audit services, and Control Implementation Services. I performed IT control reviews to assist the CPA audit staff in determining the level of reliance that could be placed on an audit client's information technology systems to plan the scope of annual financial statement audits for AICPA SAS #55 compliance. Assistant District Systems Examiner - 11th District (California, Arizona and Nevada) Federal Office of the Comptroller of the Currency - San Francisco, CA 1986 to 1989 OCC), San Francisco, CA Assistant District Systems Examiner - 11th District (California, Arizona and Nevada): I was a manager of a department of 7 federal bank examiners that were responsible for conducting Federal Financial Institutions Examination Council (FFIEC) bank information technology examinations of Savings and Loans and their IT service bureaus. I developed a risk ranking methodology to plan the annual IT examination schedule for a caseload of over 100 Savings and Loans. I managed a department of four IT systems examiners. I conducted cyber-forensic investigations of IT fraud or crimes reported to the Federal Home Loan Bank Criminal Referral Unit. I represented the federal Office of Thrift Supervision (OTS) agency at Federal Financial Institution Examination Council (FFIEC) conferences to develop new Federal Regulations. Education Bachelor of Science degree in Finance University of Illinois - Champaign, IL

Name: Brianna Schwartz

Email: jenny08@example.com

Phone: 418-222-1354x2807