

Senior Strategist - Information Security Audit Team Senior Strategist - Information Security Audit Team West Seneca, NY Work Experience Senior Strategist - Information Security Audit Team Key Bank August 2016 to Present Represented the Audit Department on legacy First Niagara technology decommission work streams. Acted as a quality assurance point of contact for audit issue closure verification, ensuring testing, documentation, and conclusions drawn by peers were up to departmental standards. Assisted other technology audit teams in completion of their audit goals when behind schedule, or short staffed. Planned and executed information Security audits based on inherent and residual risk, along with considering multiple levels of impact based on possible control deficiencies managing to a specified timeline for completion per the audit plan. Communicated audit results, conclusions, and recommendations to Bank management up to and including the CIO and external regulators. Championed a project to analyze risks, controls, threats, and vulnerabilities across multiple platforms, applications, and infrastructure within the Bank. Sat as a nonvoting member of the technology subcommittee of the enterprise risk committee to gain insight to security initiatives and risk from the view of the lines of business. IT Audit Manager, Vice President First Niagara Bank September 2015 to August 2016 Worked with Audit Directors and Chief Audit Executive to develop audit risk profiles for auditable entities, which drives the annual risk based audit plan. Planned and directed the activities of senior and staff auditors to ensure all assigned audits are appropriately staffed, planned, and executed timely. Managed multiple concurrent audits to ensure work performed was within scope, delivered on time, and to departmental standards. Consulted on integrated audits to provide insight on IT related risk within the environment. Coordinated audit activities with the Bank's external audit firm for audits where FNFG Audit work was to be leveraged by the external auditor. Communicated audit results, conclusions, and recommendations to Bank management, the Audit Director, and the Chief Audit Executive Directed and coached senior and staff IT auditors on appropriate test approach and acceptable risk tolerance within the environment to achieve audit objectives. Fostered relationships with technology, functional, and business groups within the bank, to allow for a team approach for the implementation of audit recommendations. Sr. IT Auditor, Assistant Vice President

First Niagara Bank July 2013 to September 2015   Planned audits based on inherent and residual risk, along with considering multiple levels of impact based on possible control deficiencies. Reviewed Windows Server 2003 and 2008, SQL Server 2000 and 2005, along with network infrastructure, integrated, distributed and mainframe applications for secure configuration and compliance with published standards.   Fostered relationships with technology, functional, and business groups within the bank, to allow for a team approach for the implementation of audit recommendations.   Executed audit programs, and managed a time budget to meet a specified deadline for completion per the audit plan.   Made recommendations to improve bank wide IT controls to middle and senior management.   Managed and supervised one to two staff or senior auditors on various engagements, ensuring their work was completed on time and to audit standards.   Worked with external regulators audit functions performing work on their behalf within the Bank, including but not limited to SOX 404 testing.   Acted as interim IT Audit Manager during departmental staffing changes for a 2 month period prior to formal promotion. Information Security Analyst Catholic Health June 2010 to July 2013   Drove the selection, testing, and implementation process for an enterprise Data Loss Prevention (DLP) program.   Made recommendations to improve system wide IT controls to senior management, up to and including the CIO on a regular basis.   Developed an audit schedule based on application data criticality, risk, and known issues. Planned audits based on inherent and residual risk, along with considering multiple levels of impact based on possible control deficiencies.   Worked with the network engineering team, as well as multiple vendors and business areas to enhance enterprise system security.   Implemented a policy and procedure to integrate into the enterprise change management process requiring audits of servers against a gold build prior to production promotion.   Drove the vendor selection process for an encryption solution to be implemented system wide based on a defined set of criteria and budget.

Worked to enhance the current information technology policies, procedures and standards, as well as develop new policies and standards to protect PHI and PII.   Regularly audited Windows Server 2003 and 2008, SQL Server 2000 and 2005, along with network infrastructure, integrated, distributed and mainframe applications for secure configuration. Made recommendations to enhance

the overall security posture within the Catholic Health System. Developed and implemented a process to approve and track applications that did not meet published internal standards and industry best practices with regard to security configuration. IT Audit Supervisor, Banking Officer M&T Bank June 2007 to May 2010 Planned audits based on inherent and residual risk, along with considering multiple levels of impact based on possible control deficiencies. Typical scope included security controls (app, OS, and database), backup and recovery, vendor management, and change management processes. Developed and executed the audit for the Bank's new Active Directory infrastructure. Developed understandings of complex technology platforms and infrastructures, evaluating application integration along with identified controls for effectiveness. Executed audit programs, and managed a time budget to meet a specified deadline for completion per the audit plan. Made recommendations to improve bank wide IT controls to middle and senior management.

Managed and supervised one to two staff and/or assistant supervisors, ensuring their work was completed on time and to audit standards. Participated in the annual SOX 404 audit execution, as well as understanding and reviewing the Bank plan for PCI compliance. IT Auditor Blue Cross/Blue Shield January 2006 to June 2007 Participated in FY2006 Risk Assessment and planning of the master audit plan. Developed Audit Programs for audit work based on CobiT frameworks.

Performed audit work, including research, testing, documentation of findings, and review of final audit reports based upon IIA standards. Made recommendations on improving internal controls based on industry best practices, along with current laws and regulations (HIPAA compliance, etc).

Gained big 4 audit planning, execution, and reporting experience from Ernst and Young through a co-sourced arrangement. Tier 2 Tech Rep Localnet May 2004 to January 2006 Handled inbound calls from dial-up internet service customers providing technical support. Assisted level 1 technicians with more complicated issues escalated for further troubleshooting. Mentored new techs on how to handle calls, difficult customers, and manage call times. Education Bachelor of Science in Management Information Systems in Management Information Systems State University of New York, College at Fredonia - Fredonia, NY July 2004 Certifications/Licenses CISA CISSP MCTS Present Active Directory

Name: Shannon Mitchell

Email: cassandra08@example.com

Phone: 636.422.5724x05846