IT Compliance Analyst IT Compliance Analyst IT Compliance Analyst - Barneys New York Parsippany, NJ Over eighteen years strong Information Security Program Management experience within Investment Banking and Retail industries. Skilled in identification of risk remediation areas. Adept at presenting security metrics in meaningful fashion to identify areas of potential risk. Proficient in writing and revising security policies and procedures. Quickly grasps project objectives and adopts new skills accordingly. Outstanding communication skills.   Strengths Include - Policy - Procedure - Change Management - Metrics - Monitoring - Incident Management Work Experience IT Compliance Analyst Barneys New York - Lyndhurst, NJ May 2011 to Present Manage change control process and ticketing solution. Manage file integrity monitoring solution. Conduct internal PCI audits and work with application owners to ensure compliance. Manage annual third-party internal and external audits and work with appropriate business areas to remediate findings. Maintain, modify and propose security policies and processes to reflect current regulatory and business requirements. Recommend new security tools to fit current business needs. Act as liaison between business areas and external audit teams. Coordinate annual user access recertification and facilitate changes as needed. Maintain list of security standards for installed operating systems based on industry best practices. Manage security awareness and education platform to ensure all users are well versed in company information security practices. Information Security Analyst Pershing - Florham Park, NJ May 2010 to February 2011 Coordinate quarterly vulnerability assessment for internet facing applications. Retest findings to verify remediation. Work with application development teams to remediate findings. Participate in weekly conference calls for project approval. Coordinate transition of production server management from developers to server group. Develop and execute tabletop exercise to test incident response of application business owners. Information Security Analyst NYCERS - New York, NY April 2009 to May 2010 Develop and implement security policies and procedures. Develop security risk assessment and gap analysis scenarios to identify security weakness and mitigate risks. Facilitate access control procedures for agency authentication processes. Create plans and perform security audits and vulnerability assessments to identify and enforce internal security controls. Perform complete security analysis and technical tasks involving

security measures focusing on specified /defined environments. Implement and support information security solutions including security architectures, change management and integration of security products. Information Security Analyst Bear Stearns & Co., Inc - Whippany, NJ August 1999 to November 2008 Performed periodic vulnerability assessment of internal and external applications. Identified actual application vulnerabilities and recommended remediation. Reviewed ISACA and CERT vulnerability alerts for relevance to the business. Performed security assessments of applications and partnered with application owners to secure the applications for production. Performed troubleshooting and bug fixes for security monitoring technology. Executed emergency remediation plans where metrics or incidents indicated action was required. Managed annual independent penetration study of internet facing applications, including selection of vendor, review of reports and oversee remediation of findings. Assembled, catalogued, aggregated and devised data visualization techniques for security metrics. Assisted in identification of new metrics. Assisted in selection and training of new IT Security staff.   Selected Accomplishments: Managed annual vulnerability assessment of Internet facing applications which resulted in timely identification and resolution of security vulnerabilities.   Evaluated and deployed desktop surveillance product for logging activity of consultants dealing with sensitive information. Project completed within timeframe.

  Participated in IT Security Review process for several technologies within firm. Assessed risk of these technologies and recommended action for implementation.   Evaluated and deployed instant messaging logging software for capturing Internet chat logs of broker/client communication. Conducted and facilitated the collection of data for security and legal investigations. Responded to security incidents and determined proper course of action.   Supervised audit remediation activity on annual basis to comply with SOX policies. Passed all audits satisfactorily. Education BS in Computer Science Seton Hall University - South Orange, NJ 1999 Skills Nessus, Nmap, Tripwire, Cisco, Firewalls, Cyber Security, Network Security, Information Security Additional Information Technical Skills   Programming Language: Perl, HTML, CSS, Basic, Pascal, Java, Scheme, Prolog, UNIX k-shell, C/C++, Expect, Windows batch scripting   Applications: Firewalls (Cisco, PIX and Fortinet), ChangeGear, nMap, Nessus, Tripwire 8.5, Dell KACE, Kaspersky Security Center, Trend

Deep Security, Solarwinds LEM, Microsoft EOP, Wombat/Proofpoint   Operating Systems: Windows, UNIX, Linux

Name: Shannon Schwartz

Email: melissafloyd@example.org

Phone: +1-834-961-6246x28026