Business Unit Security Officer (BUSO) Business Unit Security Officer (BUSO) Business Unit Security Officer (BUSO) - John Hancock Shrewsbury, MA An experienced and transformative cybersecurity manager with vast knowledge in leading information security, vendor management and compliance initiative. Adept at directing multi-national teams and valued for creativity, technical acumen and business-positive approach to information technology risk management. Able to translate complex security concepts into 'take homes' for non-technical audiences. Signature Achievements: Led and influenced the modernization of a struggling risk management team into a forward looking and agile minded advisory team. Significantly reduce the cost of PCI compliance assessment by 40% through an integrated compliance approach. Work Experience Business Unit Security Officer (BUSO) John Hancock - Boston, MA June 2016 to Present Lead and manage business units' cybersecurity, resilience and governance initiatives as part of Sr management 2nd line Assurance functions (COSO Framework). Develop business case justifications and cost/benefit analysis for technology spending and initiatives. Led the implementation of a new cybersecurity framework based on the COSO framework into agile value streams, Lead significant initiatives (ApigeeRobotic Process Automation, Big Data, DevOps, Blockchain, SOA-to-Microservices) and product risk assessments from a technical security and information risk management perspective (includes risk identification based on information criticality through to control implementation and management of risk acceptance by product owners and business areas.

Identify enterprise trends, synergies, and opportunities to strategically provide management assurance. Serves as cybersecurity advisor and partner to IT, product owners, release train engineers and scrum teams. Oversee the secure design and development of security features, solutions and products for insurance value streams. Provide security assessment on security architecture and requirements related to web applications, cloud integration and migration. Provide coaching, mentoring and security expertise for development teams. Develop an information security risk portfolio for the squads, initiatives and value streams. Support operational security activities including oversight of ongoing divisional security processes (e.g., incident response, ad hoc queries, periodic access reviews, and vulnerability management). Elicits and translates business requirements to systems specifications for securing complex business systems. Ensuring security specifications align with Global information security policies and standards. Review existing architecture and makes recommendations on security controls. Incorporate secure design principles and architecture level security concepts. Provide security guidance to business units migrating workloads to Azure, AWS, and Google cloud services. Assist architects in developing an aligning architecture framework with business requirements. Sr Consultant Controls Assessments and Monitoring CVS Health - Woonsocket, RI May 2015 to June 2016 Successfully completed "Report on Compliance" for PCI DSS level 1 certification for 2019 and received our "Attestation of Compliance" from the bank. Manage, facilitate, prioritize and ensure completion of information systems assessments. Interact with management to determine the scope and content of audit compliance review, consistent with department goals. Develop, identify and review organization PCI assessment scope. Track and identify PCI DSS changes that could impact the organization. Identify and review PCI assets classification and inventory. Review any significant changes to processes, applications, systems, network, technologies and its impact on PCI compliance. Review compensating controls from previous assessments. Manage and track external PCI web application (Qualys) scans. Developed a holistic Arcsight log review process in compliance with PCI DSS. Manage and complete ad-hoc reviews and departmental initiatives as requested by management. Create, track and review GRC Archer assessment requests and evidence for PCI assessment and controls monitoring. Identify risks and assess existing/proposed controls associated with information system strategy. Review PCI vendors risk profiles. Assist in the implementation of a firewall review process. Determine corrective action(s) by soliciting client recommendations and responses to the issue. Review and update security policies, procedures, and standards. Glenn Burnie, MD (Contract) Motor Vehicle Administration July 2014 to April 2015 Sr/Lead IT Security Specialist Lead motor vehicle administration PCI and state compliance program. Coordinate external and internal penetration test with vendors. Lead and track remediation of penetration test findings. Created a PCI log review procedure. Developed threat and vulnerability management procedure and standard. Track vulnerability profile of the MVA.

Manage and track PCI safeguard implementation guide (SIP) register.   Review MVA standards, procedures and policies.   Conduct internal audit of MVA servers.   Provide information security guidance and counsel to the CISO, PMs, and IT director.   Lead and manage MVA security incidents and events from Qradar SIEM.   Implement and lead MVA McAfee data loss prevention (DLP) project.   Review data loss prevention incidents with stakeholders.   Train MVA employees on the functionality of McAfee DLP.   Lead the implementation of Tripwire file integrity monitoring. IT Risk Manager (Threat &Vulnerability Management) JP Morgan Chase, Delaware December 2012 to May 2014   Manage, and revamped threat vulnerability management process.   Provide support throughout the lifecycle of various audits.   Provide control consulting on emerging risks and key initiatives (Cyber and IAM)   Supports CIO to ensure they are addressing current and emerging risks.   Collaborate with enterprise architecture to reduce cyber security risk of the business units.   Responsible for providing Risk Management support across the CCB lines of business.   Provide risk guidance in the remediation of issues and action plans.   Work with global operations management to promote risk awareness and compliance across lines of business.   Manage and conduct adhoc audit, compliance assessment and any audit related projects. Sr Information Security Analyst Jos A. Banks - Hampstead, MD April 2009 to December 2012   Conduct and develop remediation process for PCI audits with Plan of Action and Milestone process.   Documentation of enterprise daily logs as required for compliance with PCI DSS.   Assess enterprise information systems internal controls as required by PCI DSS.   Conduct SOX quarterly user audit.   Managed and perform organization wide quarterly users and systems audit.   Audit enterprise application using IBM BigFix reports.   Review and update security policy, procedures, standards and guidelines.   Monitor, research, and document Dell Secureworks IDS network alerts/logs.   Monitor and respond to McAfee SIEMS alert.   Monitor and review McAfee ePolicy Orchestrator malware alerts.   Educate staff and organization about new threats and breaches through emails and newsletters.   Research and identify security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives. Security Engineer McAfee Suite Department of Commerce - Silver Spring, MD January 2008 to April 2009   Maintain FIPS compliance systems using McAfee ePolicy Orchestrator 5.0. Assisted the agency in meeting Cyberscope goals by encrypting 1500+ machines using McAfee endpoint encryption. Automate, create and deploy antivirus DAT files to systems using ePO server. Create weekly patch and vulnerability reports. Learn and Experience. Systems Administrator Xerox - Columbia, MD February 2005 to January 2008 Automate the deployment of encrypt to systems using McAfee ePo. Deploy enterprise windows updates, patches and critical security application using SCCM package manager. Manage and deployed system images using tools such as SCCM, Norton ghost. Developed mitigation strategies to harden offsite systems. Audit and remove unapproved software from environment. Education Bachelor's in Bus IT Management WGU - Salt Lake City, UT January 2018 to Present

Name: Mark Harrison

Email: danieltaylor@example.net

Phone: 578.440.1268x430