Contract Senior Information Security Compliance Consultant Contract Senior Information Security Compliance Consultant Dr. of IT and Cybersecurity Assurance that will help you exceed your compliance goals..and I'm pretty cool. Hillside, IL Doctor of IT Security offering over 15 years experience in IT Compliance Leadership from a combination of private sector, academics, and government practice. Consistently recognized for process improvement strategy used to cost-effectively resolve challenging compliance alignment (PCI,SOX,,HIPAA,etc.) Create and foster Joint team efforts across business units to significantly reduce process time and expand innovation think pools. The result is faster, pioneering solutions for the organization by the organization. Authorized to work in the US for any employer Work Experience Contract Senior Information Security Compliance Consultant Allstate Insurance - Northbrook, IL May 2019 to Present Responsible for assisting in driving the company s efforts to proactively identify, assess, and communicate the company s information security risks through critically analyzing the probable frequency and probable magnitude of future loss. The assessor works in close partnership with internal information security and business representatives to scope assessments, gather documentation, interview clients, identify risks, document findings, and ensure transparent management of risks by following a structured risk assessment methodology. Successfully independently lead and complete high-quality assessments across a diverse set of technologies, business functions, and complexity. This includes but is not limited to assessments for internal and SAAS applications, network devices, control processes, business functions, and facilitating the ongoing analysis of enterprise-wide risks across Allstate and its family of companies. Streamline processes by partnering with management and team members to proactively identify and participate in implementing process improvements, overcome barriers to success, build professional relationships across the company, brief senior leaders, and be a collaborative member of the team. Works closely with and influences decision makers in other departments to identify, recommend, develop, implement, and support a risk informed decision and action framework to successfully support the business by streamlining the decision makin process by 20 percent average. Change Catalyst for a risk based approach to delivery of services and systems by partnering with others in

their organization to set and manage expectations; continually seeks opportunities to be a thought partner and increase internal business partner satisfaction and deepen relationships. Adapts communication approach for audiences at multiple internal and external levels. Identify and recommend appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to a level acceptable to the senior management of the company. Identify and report on new and emerging security risk and risk trends, including participating in risk remediation solution discussions and updates to compliance policy and standards. Fully understand business requirements and work with the business to define appropriate solutions for security objectives while meeting the business need. Manage the review of changes in company processes, standards and technology to ensure the effectiveness of security controls to meet compliance requirements. Integrate security risk reporting and management activities into Allstate day to day processes. Partner with all areas of the business, including internal auditors, legal, IT and business partners. Respond to and assist with audits, assessments and compliance requests. Serve as client liaison as needed on matters pertaining to Risk Management. Promote and consult on the positions that help strengthen and secure the organization by either following standards or helping direct others on technology positions. Act as a subject matter expert for the organization's information asset protection policies and procedures, and information technology best practices. Develop and refine enterprise policy, standards, procedures, and techniques used by the team to improve operations process time by 50 percent. Help facilitate assessment reviews of individual business unit and/or supplier compliance to above leveraging manual questionnaires and/or Archer GRC compliance module. Assist in identification and reporting of compliance gaps to key stakeholders for remediation actioning by creating customer executive level summaries. Help identify all instances of overlapping questionnaires within silo compliance program efforts (SOX, PCI, HIPAA, state regulations, etc) to improve partnership and collaboration Help define Common Control framework capability in Archer GRC to cross map a set of controls to the requirements from different regulations and standards. Ultimate objective is that once a control is tested, the test results can contribute to the assessment for multiple regulations and standards without duplicating work.

Support team members and business processes managing the lifecycle and inventory of critical technology assets (monitoring, enumeration and classification of various regulatory and compliance information assets) Compliance program support (PCI, HIPAA, NYDFS, SOX, SEC / GLBA), scope management, along with 1st level triage of consultative requests (engaging lead consultants as required and when appropriate), and supporting supplier compliance reviews Consult with stakeholders and/or suppliers on requirements for new and existing business / technology solutions to assure compliance to applicable regulatory or contractual control requirements (ex. PCI, HIPAA, state regulations, internal standards and governing policies and procedures) Associate Director- IT Security and Compliance Publicis Groupe - Chicago, IL March 2016 to February 2019 * Lead security team to successfully reduce security risks and enhance IT security compliance. * Successfully manage billion-dollar projects to maintain IT Security Program for ISO27001 alignment for globally. * Reduce employee turnover by 50% by developing team "positive insights" strategy and concepts that results in a enhance positive work environment that supports award winning innovation and solutions. * Lead team to develop strategies and concepts that result in rapid compliance alignment of newly acquired business partners. * Create IT Security policies to improve alignment of new technology and processes, resulting in improvement of executive management strategy development. * Create cloud services documents (PaaS, IaaS, Power BI, Microsoft, etc.) to maintain and enhance compliance alignment to global rules or regulations. * Review new technology as part of executive IT security approval board resulting in secure assimilation of technology for over 30% reduction in integration time of projects. * Consult and assist in creating programs necessary to achieve federal/state regulations or compliance with practices such as ISO27001, SSAE18 and comparable best practices. * Manage, execute, and streamline audit requests by collaborating with executive and business units resulting in improved client satisfaction as well as compliance for multi-million-dollar accounts. * Foster and improve positive culture by creating team events and synergy exercises. Presented and educated management on positive reinforcement strategy to improve positive work environment and employee empowerment. * Create Risk Assessments to improve security controls resulting in 30% improvement in compliance

alignment time. * Improve team knowledge by over 50% by streamlining training budget expense for IT security industry certifications and training to allow for more training opportunities. * Create communication report using advance MS Office techniques for executive management to improve management and team communication of strategies; result is a streamlined executive management decision process. * Advise and collaborate legal team as IT security expert for client negotiation; resulting in more than a 50%-time reduction in contract signing. * Develop Security Awareness program to improve employee recognition of security concepts globally. * Improve security awareness of organization by addressing security and compliance requests along with security questions * Increase organization client sales operation process by 40% by reducing time for contracts and negotiations by answering security assessments, performing audit requests, and addressing any security compliance requests. Officer Army National Guard - Springfield, IL August 2010 to August 2018 * Secure the Largest network in the world (DoD) by directing employees involved with the application of electrical, electronics, and systems engineering. * Management of multi- million in technology assets * Insure IT processes follow state/federal laws by strategically implementing unique frameworks based on the IT process meeting lawful requirements (USA Patriot Act, AML, BSA, and OFAC.) * Manage over 35 employees in the design, test acceptance, security, installation, operation, and maintenance of IT systems, equipment, networks, and facilities. * Conduct risk assessment to reduce injury and increase efficiency in team operation. * Conduct audit on Cisco Routers, Switches, VPN, and other related IT devices for information assurance. * Investigates or oversees the investigation of losses and security violations and recommends corrective actions. Implements approved course of action as appropriate. Provides summaries for senior management review. Toys R Us - Marion, IL (Temporary work completed while attending university-SIUC) * Completed IT audit which effectively decreased employee data error 50% resulting in savings of 20k by removing outdated employee information. * Managed associate data management processes (PeopleSoft, PTO, ETOI management, LOA and eRoster) to improve allocation of resources in Fortune 500 Company by reconfiguring the automated workload system during HR compliance audit. * Assure that organization has met federal/state laws by monitoring

through compliance, risk management, and audits using Understanding of current regulatory environment and related implications to identity management and security/audit compliance * Assisted the Regional HR Director with company strategy to promote a positive internal culture within the organization by adhering to government regulations and paperwork. * Reduced employee turnover by 25% with implementation of intrinsic/extrinsic reward IT Security Consultant Discover Card - Wall Street, NY June 2015 to September 2015 6/2015-9/2015) * Created IT Security Policies for the organization resulting in increase of Security awareness by 70%. * Successfully aligned policies to SOX and PCI standards in order to initiate global alignment of organization to the IT governance needs. * Assist Information Security Program Office (ISPO) as a Subject Matter Experts (SME) on IT security compliance and best practices in order to significantly improve alignment organization with IT governance strategy * Developed business unit collaboration as a liaison between business and IT; bridged the translation gap to identify organizational needs for IT and business * Advise upper management on upcoming or potential threats using security in order to decrease the chance of a security breach * Directing application security procedures through compliance, risk management, and audits. * Lead security team to successfully reduce security risks and enhance IT security compliance. * Successfully obtain buy in from executive management based off professional presentation of governance strategy using advanced features of Microsoft excel and word. * Consult all department areas as a SME in order to successfully align banking organization with PCI and SOX requirements. * Consult and assist in creating programs necessary to achieve federal/state regulations or compliance with practices such as PCI, ISO27001, SOC2 and best practices. * Advise IT governance boards on the best course of action for security concerns or new or existing project and applications resulting in decrease of security risks IT Security Policy Engineer Kirkland and Ellis - Chicago, IL October 2014 to February 2015 * Successfully meet milestones and deadlines through constant communication of created project management risk estimates (Gant charts, diagrams, Eclipse Project Software). * Decrease system vulnerability creating Group Policy for service accounts using Spec Ops application. * Conduct monthly vulnerability meetings to harden enterprise systems. * The successful Liaison between business

and IT; bridged the translation gap to identify organizational needs for IT and business. * Design Security Awareness Program for Year to decrease risk of vulnerability in the organization using various communication channels * Researches technological advancements to ensure that security solutions are continuously improved, supported and aligned with industry and company standards. * Consult SMEs how to incorporate IT security standards into applications to meet HIPPAA, SOX, and PCI regulations. * Update Policy for organization to align with business and Security needs. Contract Information Security Engineering Consultant CVS - Buffalo Grove, IL March 2014 to October 2014 * Successfully aligned Adjudication management department with governance regulations such as HIPAA, SOX, and PCI; by Consulting IT management and Subject Matter Experts (SME) on IT security compliance and best practices. * Create pivot tables or charts to present high level summary to executive management in order to assist upper management into making the best decision on corporate IT strategy. * Successfully meet milestones and deadlines through constant communication of created project management risk estimates (Gant charts, diagrams, assessments). * Train SMEs how to incorporate IT security standards into applications to meet HIPAA, SOX, and PCI regulations. * Create policy and procedures to meet needs of business and IT governance. * Create SharePoint forum for a knowledge repository for answers to Archer risk management, Security Risk documents. * The successful Liaison between business and IT; bridged the translation gap to identify organizational needs for IT and business. * Identified and justified risk remediation with the risk remediation board to exceed compliance goals. Cyber Security Analyst ACET-Adams Communication and Engineering Technology - Hines, IL March 2013 to March 2014 * Support the VA Office of Information & Technology (OI&T), Office of Information Security (OI&S) Enterprise Operations Center Support (EOCS) to maintain secure operations on the 2nd largest network in the U.S. * Increase efficiency of team security analysis by min 25% by assuming role of Subject matter expert. * Provide the support of VPN technology, intrusion detection, prevention, incident response/recovery, and antivirus support; strong understanding of Windows and IP networking. * Expert use of Splunk, SourceFire, Siteprotector to analyze, report events to executive management ,and resolve key issues. * IT Security Incident Management,

Resolution, and Representation & Collaboration with other VA entities, and especially the Tier III layer. * Assure that the organization has met federal/state laws as well as business requirements by directing application security procedures through compliance, risk management, and audits. Information Security Compliance Administrator Advanced Technology Services - Schaumburg, IL April 2011 to March 2013 Provide IT Consultation for fortune 100 organizations such as Kiewit, Sears, Fuji, Caterpillar, Motorola Solutions, Motorola Mobility and BorgWarner resulting in enhance IT security compliance alignment across various industries. Duties consist of Server Management, active directory, security analysis, compliance monitoring, and process improvement. Oversees the development and implementation of corporate-wide application security procedures in client environments by developing identity management strategies and architectures Establish data Assurance by implementing point to point encryption (Media encryption, PKI) as well as hardware embedded encryption. Assure that organization has met federal/state laws as well as business requirements by directing application security procedures through compliance, risk management, and audits. Oversees the implementation of appropriate access controls to ensure that access to systems, data and programs is restricted to authorized and trained users. Oversees the destruction of highly sensitive confidential information in accordance with policies and procedures. Serves as a subject matter expert concerning system solutions, security procedures and audit compliance by providing leadership and work guidance to less experienced personnel. Coordinates sensitive aspects of corporate security programs to ensure compliance with client, government and company security policies and procedures including verifying adherence to specific policies and ensuring policy compliance with government regulations. Investigate and oversees the investigation of losses and security violations and recommends corrective actions. Assist in the selection and tailoring of approaches, methods and tools to support service offering or industry projects Researches technological advancements to ensure that security solutions are continuously improved, supported and aligned with industry and company standards. Capella University August 1994 to March 2011 Selected Contributions: * Researched and developed knowledge-base Information Technology articles for Capella University. * Assist the village of Joliet in the strategic

planning of streamlining the streets, surveillance, and transportation systems resulting in savings of 75k.Focused on bridging the gap between business and IT by constantly utilizing Performance Improvement. * Improve community IT operations (neighbors, family, friends, and local church) by 90% through step-by step technical support and hands-on work. Education Doctor of Computer Science in Information Security and Assurance Capella University - Colorado Springs, CO Master of Business Administration in Business Administration Human Resource Management Devry-Keller Graduate School of Management Bachelor of Science in Liberal Arts/ Business Systems Southern Illinois University - Carbondale, IL Associates in Applied Science in Applied Science Triton College - River Grove, IL Skills Cissp, It Security, Hippa, Information Security, Cobit, Cisa, Fisma, SOX, Compliance, Nist Military Service Branch: United States National Guard Rank: 1LT Publications The Mhealth Wireless Technology Adoption of the Nurse Practitioner 2018-10 The Mobile Wireless Technology Acceptance Model (MWTAM), a variant of TAM, was used as a tool to measure factors that affect the behavioral intention of the nurse practitioner to adopt mobile health (mHealth) wireless technology in their environment. MWTAM consist of the constructs of technological influence processes and cognitive influence processes. The constructs of the technologoical influence processes are perceived ubiquity and perceived reachability. The constructs of the cognitive influence processes are job relevance, perceived ease of use, and perceived usefulness. Technological influence processes and cognitive influence processes are reviewed for their impact on behavioral intentions. The variables where placed into individual hypothesis and assessed for the impact on wireless technology adoption represented by the dependent variable behavioral intention. The constructs of MWTAM were presented to a minimum of 150 participants in the form of 22 questions.

Name: Sean Mann

Email: darrell12@example.org

Phone: +1-450-466-6276x09786