

## PROFILE

With over 19 years of experience supporting global clients on information security, information risk management and data privacy challenges, my expertise ranges from identifying client challenges to providing recommended solutions to implementing those solutions. These projects were managed with diverse, global teams with the intent toward making the client self-sufficient in maintaining the implemented solution.

In addition to my current work with Multi-National Banking Agencies, I have served as Deloitte's Lead Security and Privacy Services Principal for the U.S Department of Homeland Security and the U.S. Department of Justice where I focused on cybersecurity at the programmatic and network levels as well as at the operational level with activities such as: intrusion detection; enterprise security architecture; user provisioning; secure messaging; web access management; and secure Wide Area Network (WAN) access control.

I am a Certified Information Systems Security Professional (CISSP) with an advanced certification as an Information Systems Security Management Professional (ISSMP). I hold the Certified Information Security Manager (CISM), the Certified Information System Auditor (CISA), the Certified Information Privacy Professional (CIPP/G) with advanced certification in US Federal Government Privacy and the Certified in the Governance of Enterprise Information Technology (CGEIT) designations. I hold a BS from Penn State University and a MBA in Strategic Planning from University of Pittsburgh. I have published works on enterprise security programs and information protection as well as led various industry panel discussions on information security, data privacy and identity management. Lastly, I am the National Deloitte Leader for the International Business Resources Group, which is part of our Diversity & Inclusion initiative, whose mission is to promote cultural diversity and understanding across all aspects of Deloitte.

## PROFESSIONAL EXPERIENCE

### *Principal*

*Deloitte LLP - San Francisco, CA and Washington, DC*

*04/00 - Present*

- *Multi-National Banking Agency* - leading an information protection assessment for over 250 business processes as well as supporting the IT Costing Model project in an advisory capacity. The information protection assessment involves rationalizing and assessing the data controls for the current business processes; assessing and providing recommendations associated with a proposed Information Classification Model based on the entities' disclosure and current classification models; developing and recommending a baseline set of data handling requirements (security and privacy) in accordance with WBG policy and national data protection laws from the European Union, Asia, the Americas and generally accepted security standards such as ISO27001. In addition, I am working with the Office of Information Security (OIS) to develop and implement the information classification and IT asset management handbooks through consultation with Information Technology (IT), disclosure policy and legal stakeholders.
- *Multi-National Banking Agency* - led an information security program assessment that culminated in an information security improvement roadmap, which outlined several key initiatives. Implemented several of the key initiatives including: developing information security training for the Information Technology Coordinators (ITCs) for the Country Offices (CO); conducting solution assessments for End-Point Protection and Full Disk Encryption; rationalizing current information security procedures with the ISO 27001/27002 standards; and supported the development of a Service Level Agreement (SLA) for information security services between the OIS and agencies' information security group. Currently, working to develop enterprise roles and a role management process in order to support user access management for Internal Control over Financial Reporting (ICFR) readiness.
- *U.S. Healthcare Insurer* - managed the architecture, design, testing, and operational turnover of an 18-month, \$20 million comprehensive enterprise-wide security infrastructure program that met federal security and regulatory requirements and resulted in the successful, on-time and within budget implementation of the following solutions: logging and monitoring - intrusion detection; enterprise security architecture; Internet firewall access control; user provisioning; secure messaging; web access management; and secure WAN access control.

- *U.S. Healthcare Insurer* - implemented and maintained a Security Infrastructure Program Management Office (PMO) that was responsible for the security project lifecycle, change management, operating system (OS) hardening, issue resolution, procurement, standard project documentation, and reporting. Established and managed a core development team of 18 individuals and cross-organizational teams to support the execution of 8 concurrent projects; and delivered periodic reports to senior management about project status as well as capital and expense budget status.
- *Major U.S. Federal Department* - Led the evaluation of the maturity of the Department's IT security program, provided recommendations for improvement, and developed an action plan based on the selected recommendations. For this evaluation, developed a Capability Maturity Model-based framework to evaluate the security program using consolidated requirements from NIST, FISMA, OMB A-130, FISCAM, and ISO 17799:2005. Implemented several of the key recommendations such as: designed, developed, implemented and maintained an Information Security Risk Management Council which included representatives from both the Department headquarters and the 27 individual agencies; developed the scope of operations, services definitions, services roll-out and implementation plan for its security operations center; and developed a Certification and Accreditation (C&A) process to rationalize and reduce the number of applications reviewed on an annual basis to met regulatory requirements and to reduce overall C&A hours and costs for the organization.
- *Major U.S. Federal Department* - Led an effort to shape a major United States Federal Department's strategy for data protection and data handling, which included developing a toolkit to help business process owners document and analyze the life cycle for all business process supporting data elements. This toolkit allowed business process owners to identify data risks and recommend potential safeguards to remediate these respective risks. In addition, developed a strategy to enhance the organization's policies and training capabilities to appropriately capture proper data protection and data handling requirements and concepts. Developed a security and privacy approach and handbook for implementation of services in support of one its key agencies' SOA environment including an approach for SOA C&A. In addition, developed an approach and implemented a pilot for identity management for the SOA environment. Finally, based on the Department, agency and commercial privacy and security requirements developed a privacy system to work in conjunction with one of the Port Security Card program implementation. The implementation focused on data handling policies and procedures, incident response, and help desk support for card management.
- *Global Life Sciences Corporation* - Performed Sarbanes-Oxley Act of 2002 ("SOX") readiness and assessment activities that assisted the company in preparing for its certification. Specifically provided Project Management Office (PMO) support including status and deficiency tracking, supported risk assessment workshops to review business processes and IT systems risk rating, supported controls validation & optimization workshops with key business owners to review and update the SOX internal controls, assisted management in responding to external auditor questions by providing clarification regarding actual testing performed and results of testing, and implemented a Global Education and Awareness program to address SOX remediation efforts, SOX readiness and assessment activities in the United States, Asia and Europe and address 13 different foreign language requirements in order to meet the following objectives:
  - increase enterprise-wide awareness regarding the significance of Sarbanes-Oxley regulation;
  - increase the flow of financial accounting information into the Controller and Corporate Finance from individual business units and operations; and
  - reduce the number of post-close adjustments and control deficiencies identified in fiscal year.
- *Global Clothing Manufacturer* - conducted an information security environment analysis for the company's global information security program, which produced the following: future state information security program, based on leading practices and ISO 17799, which resolved audit findings and aligned with business strategic initiatives; prioritized roadmap and budget for the implementation of the future state environment and implemented several of the initiatives, which included the following:
  - An IT risk management process based on ISO17799 that leveraged current business processes;
  - A security awareness program to support end user information security awareness; and
  - A security architecture including a process for documenting "reusable" security requirements for the components of the IT infrastructure (e.g., Enterprise Applications) and procedures to manage requirements on a periodic basis.

## Brian T. Geffert

---

- *Major Financial Institution* - developed an IT governance framework for a financial institution that had outsourced its core application development and maintenance functions. The framework was based on generally accepted standards and practices (COBIT, ITIL, ISO), including adoption of standard enterprise IT controls.
- *U.S. Telecommunications Service Provider* - supported the implementation of role-based access controls for a PeopleSoft implementation. The support included assessing the current role design and developing the future roles needs based on the merger of two separate PeopleSoft systems into a single new PeopleSoft system. Designed and implemented TIER I and II access control help desk function to support the implementation and migration of user to the new PeopleSoft system.

### ***Manager***

***KPMG LLP - Washington, DC***

***10/96 – 4/00***

- Championed the National KPMG Health Care Incubator Effort, which integrated the development of a methodology and internal training materials for assessing a client's compliance with HIPAA security and privacy regulations. In addition, developed and executed external and internal marketing plans, which included the creation of a sales team, identifying sales channels, preparing and distributing marketing materials, and presenting at healthcare related conferences.
- Led the on-going Monitoring and Reporting Executive Committee for the HIPAA Security Summit, an industry-based working group, which resulted in the development of an implementation guide for U.S. HIPAA security regulations. Led a Forum on Privacy and Security in Health Care that resulted a cost analysis, which determined the financial effects on health care organizations, accrediting organizations, and health care solutions vendors in adopting federal security regulations.
- *Major US Federal Department* - prepared cost/benefit analysis for the implementation of Enterprise Resource Planning packages. Gathered and analyzed cost data for two different alternatives, which included in-house CASE tool development and commercial packages. Analyzed and compared each alternative to determine the most cost effective means to replace the current material management system. In addition, designed and analyzed alternatives for optimizing of their distribution system. Conducted feasibility tests and sensitivity analysis on the distribution system's cost drivers to determine their influence on the overall outcome of each scenario.

### ***Business Logistics Financial Manager***

***UNITED STATES DEPARTMENT OF THE NAVY - Washington, DC***

***09/91 - 07/95***

- Supported the development of the Annual Readiness, Sustainability & Logistics Budget (\$2.5 Billion) by conducting financial analyses, formulating alternatives, coordinating with 5 major divisions in the Chief of Naval Operations (Pentagon), and developing point papers to brief Department of the Navy Senior Management and address United States Congressional inquiries.
- Developed comparative cost analyses for the Naval Air Systems Command including evaluating procurement requirements to current dollar financial alternatives; comparing cost avoidance component costs, total costs, and logistics support estimates; quantifying costs and benefits associated with varying levels of simulation and airborne flight time; and incorporating "what if" scenarios to anticipated requirements, funding, and production variances.

## EDUCATION

- **Harvard Business School Executive Education**  
Leading Professional Services Firms Certificate, March 2008
- **University of Pittsburgh**  
M.B.A. in Strategic Planning, June 1996
- **Pennsylvania State University**  
B.S. in Finance with Distinction, May 1991

## CERTIFICATIONS

- Certified in the Governance of Enterprise IT (CGEIT) 2008
- Certified Information Privacy Professional (CIPP) with Advanced Certification in Federal Government Privacy (CIPP/G) 2007
- Certified Information Security Manager (CISM) 2004
- Advanced Certification as an Information Systems Security Management Professional (ISSMP) 2002
- Certified Information Systems Security Professional (CISSP) 2000
- Certified Information Systems Auditor (CISA) 1998

## PUBLICATIONS

- Co-Author of “Building a Secure Workforce – Guard Against Insider Threat”, Deloitte, 2008
- Co-Author of “Security and Privacy in the Agile Enterprise”, The Agile Enterprise – Reinventing your Organization for Success in an On-Demand World 2005
- Author of “Incorporating HIPAA Security Requirements into an Enterprise Security Program”, The HIPAA Program Reference Handbook, 2004
- Guest Editor, The ISC2 Journal, Volume 13, Number 5, November/December 2004
- Co-Author of “HIPAA 201: A Framework Approach to HIPAA Security Readiness”, Information Security Management Handbook - 2003
- “Using a User Account Management Framework to Protect Your Resources”; Deloitte & Touche LLP; Geffert, Kobel, and Hamburg, 2001

## PRESENTATIONS/PANELS

- Keynote Speaker, Philadelphia CSO Breakfast Club Predictions Dinner - 2009
- Speaker, Ira H. Shapiro Memorial Lecture, Fifth Annual Forum on Financial Information Systems and Cybersecurity: A Public Policy Perspective - 2008
- Moderator , Designing Secure Architectures for Business Survival, egov Institute, Enterprise Architecture Conference - 2007
- Deloitte International Assignment Services - North American Conference (Data Privacy) - 2005
- Secureworld Expo 2005: Led the Identity Management Roundtable and Identity Management Industry Expert Panel
- IAPP Truste Symposium - Security for Privacy Professionals Boot Camp - 2004
- IAPP Audio Conference Series: Outsourcing Overseas - Privacy Risks in Offshore Service - 2003
- HIPAA Security Summit West II - Pre-conference Symposia: HIPAA 2.01 For Healthcare Data Security Officers Who Don't Want to Go to Jail and HIPAA Security: A Practical Risk Based Approach - 2003

## PROFESSIONAL ACTIVITIES

- National and Greater Washington Area Deloitte Leader for the International Business Resources Group
- Board Member, United for DC, DC United Football Club's Charitable Arm