

Kim L. Jones CISM, CISSP

**14903 N. 86th Drive
Peoria, AZ 85381**

**(480) 489-2829
KLJones.CISM@Gmail.Com**

PROFILE

A 34-year innovative security, technology, and risk leader committed to continuous improvement. Recognized for process developments and improvements that have provided multimillion dollar cost reductions while increasing quality and reducing and/or eliminating risk. Track record of delivering information security solutions that meet business and customer needs. Fosters effective partnerships and engagement on information security risks on a wide range of technologies, organizations, internal, and external threats. Progressive expertise encompassing:

- Security Strategy
- Information security management
- Organization and resource planning
- Enterprise security governance
- Policy development and implementation
- Project and portfolio management
- Security and operational risk assessments
- Security risk management
- Staff development
- Business continuity planning and management
- Change and incident management
- Personnel security
- Physical security
- Quality improvement

SECURITY STANDARDS

Possesses practiced understanding of the following security standards and privacy regulations:

- Payment Card Industry Data Security Standard (PCI-DSS)
- Federal Financial Institutions Examination Council Regulations
- NIST Cybersecurity Framework
- Global Data Protection Regulation
- California Consumer Privacy Act (CCPA)
- ISO 27001/2002 (*Information Technology – Code of Practice for Information Security Management*)
- SOC 1/SOC2 Reporting
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act
- Sarbanes-Oxley Act

EXPERIENCE

Director, Security Operations

2018-Present

Intuit, Mountain View, CA

Director on Intuit's global Cybersecurity, Compliance, Risk, and Fraud Team. Responsible for all aspects of incident response; forensics investigations; and identity-related fraud operations in all geographies across all product lines.

- Codified Intuit's incident response processes, which allowed for uniform response characteristics across all business unites and geographies.
- Reduced mean time to response (MTTR) by 14% by improving the automations and technology stacks for alerts and incident monitoring.
- Led the adoption of the MITRE ATT&CK framework within Intuit.
- Created Intuit's detection tuning program, which allows us to validate the efficacy of our detection systems. Program has resulted in a 3% improvement in event detection throughout the enterprise.

Professor of Practice

2016-2018

Arizona State University, Glendale, AZ

Professor of Practice and Director of ASU's Cybersecurity Education Consortium (CEC). Responsible for developing curricula, programs, and activities designed to create high-quality cybersecurity professionals. Responsible for all aspects of CEC Operations to include strategic planning; fundraising; and course development.

- Developed Cybersecurity Concentration under ASU's Applied Computing program. Developed unique coursework; concentration proposal; and student growth projections for submission to the provost and the Arizona Board of Regents. Over 500+ students enrolled within this degree program.
- Developed and taught Governance, Risk, and Compliance courses to over 75 ASU students.
- Developed and maintained relationships with large Arizona business entities to create relationships between them and the CEC.
- Funded and developed ASU's cybersecurity curriculum for middle- and high school STEM programs. Curriculum is currently in use in over 12 school districts in Arizona.
- Raised over \$500,000 in support of CEC activities.

Senior Vice President & CSO

Vantiv (now Worldpay), Cincinnati, OH

2012- 2016

Chief Security Officer (CSO) for Vantiv, the largest PIN-debit processor and 2nd-largest credit card processor in the US. Responsible for all aspects of information security; physical security; security risk management; security governance and compliance; threat intelligence; access management; security architecture; and business continuity. Supervises a team of over 75 full-time personnel and 100+ contract guard force.

- Developed and executed Vantiv's first comprehensive security strategy, which shifted the focus of the security team from perimeter defense to business engagement and enablement. Resulting business and operational synergies helped decrease technology deployment times by 10%.
- Regularly and routinely interfaced with Vantiv executive committee and Board of Directors in order to determine/reassess security priorities in support of revenue goals.
- Developed and implemented a comprehensive security metrics program which quantified asset utilization as well as the state of security within the Vantiv network.
- Supervised development of Vantiv's target enterprise security architecture, which ensured clearly understood and measurable technical controls were present during all innovation efforts.

EXPERIENCE (cont'd)

- Developed and implemented a comprehensive skills and leadership training program for all Vantiv security personnel. Resulting improvements in team abilities helped decrease process throughput times by 4%.
- Successfully completed 22 major audits annually without significant findings or incidents.

Information Risk Manager & Deputy CISO

General Dynamics C4 Systems (GDC4S), Scottsdale, AZ

2009-2012

Information Risk Manager and Deputy CISO for GDC4S – a developer and integrator of security communication and information systems technology for the defense sector. Responsible for overseeing and implementing risk assessment, monitoring, management, and mitigation activities, including security ruleset management, incident response, security architecture roadmaps, policy management, risk assessments, forensic investigations, and security event monitoring. Supervised a team of 12 full-time personnel providing critical infrastructure protection for an 8,000+ person company operating on 2 continents and in 2 active war zones.

- Implemented GDC4S's first Information Security Risk Management Framework, allowing business units to effectively measure and balance risk versus return when making technology decisions.
- Instrumental in moving the GDC4S information security structure to a services-oriented, ITIL-based delivery model.
- Developed and implemented a comprehensive security metrics program which quantified asset utilization as well as the state of security within the GDC4S network.

Vice President & CSO

eTelecare Global Solutions, Scottsdale, AZ

2007-2009

(Company sold; position eliminated)

As Chief Security Officer for eTelecare, a contact center outsourcing company, was responsible for overseeing and implementing information security, physical security, and network security. Supervised a team of 9 full-time personnel providing critical infrastructure protection for a 13,000+ person company operating on 3 continents.

- Created eTelecare's first security organization, designed and implemented to quickly and efficiently migrate the company's security posture to a "best practices" state.
- Achieved global compliance and certification with the Payment Card Industry Data Security Standard (PCI-DSS) in all geographies and locations.
- Successfully positioned eTelecare to meet all security requirements for its first Sarbanes-Oxley audit.
- Developed and maintained a comprehensive security awareness program that facilitated a strong physical and information security posture.

Senior Vice President & CSO

eFunds Corporation, Scottsdale, AZ

2003-2007

(Company sold; position eliminated)

As Chief Security Officer for eFunds, a global financial technologies company, was responsible for overseeing and implementing information security, physical security, business continuity, disaster recovery, and network security. Supervised a team of 117 full-time personnel providing critical infrastructure protection for a 5,500+ person company operating on 4 continents.

- Developed eFunds' first global security strategy. Set specific objectives designed to enhance the company's overall security posture; obtained support, approval, and funding for execution from the Board of Directors and executive team; executed 18 major projects on time and under budget.

EXPERIENCE (cont'd)

- Improved the company's continuity and recovery posture in order to meet legal and contractual requirements. Acquired and installed over \$15 million worth of equipment on time and in a fiscally responsible manner.
- Achieved BS 7799 (later ISO 17799) certification for 6 of eFunds' overseas facilities.
- Augmented the company's security technologies such that the technology could accurately monitor the security and compliance of all network devices in near-real time. As a result, the number of security-related operational incidents decreased by over 80%.

Manager

Cap Gemini Ernst & Young (CGE&Y), McLean, VA

2001-2003

Consulting manager with CGE&Y's Security Solutions Group. Provided security consulting services to commercial clients. Assisted in development, cross-sector implementation, and cross-sector delivery of information security offerings throughout CGE&Y's North America business unit.

- Evaluated the information security policies and procedures environment for a global pharmaceuticals company against ISO 17799, providing recommendations for improvements. Results were presented during a multi-national workshop. Subsequently wrote global security policies for the company.
- Played a principal role in the development of CGE&Y's Business Continuity/Disaster Recovery offering, to include strategic market positioning, delivery methodology, deliverable construction, training plan, and staffing plan.
- Assisted in development of CGE&Y's offering to provide security services in relation to the Health Insurance Portability and Accountability Act (HIPAA). Delivered HIPAA security & privacy gap assessments to numerous healthcare payer and provider organizations.

Senior Security Consultant

ZEFER Technologies, Columbia, MD

2000-2001

(Company went out of business)

Senior Security Consultant within ZEFER's Information Security Group (ISG). Provided strategic-level information security consulting services to Global 1000 companies in multiple verticals. Services included policy and procedure creation/review; risk, threat, vulnerability, and compliance assessments; technical implementation of security products; security education and training; and strategic planning/business process reengineering for security requirements. Played substantial roles in development and codification of several ZEFER security service offerings.

- Provided enterprise-wide security and risk management strategies to Fortune 1000 companies. Translated business goals and objectives into security functional requirements, long-range security plans, and technical architectural requirements.
- Served as Director of Security Assessments for ZEFER ISG. Created and maintained assessment methodologies; developed assessment marketing strategy and materials; developed pricing model for all assessment offerings; and served as project manager of all assessments conducted.

ADDITIONAL POSITIONS HELD**Computer Security Consultant***Computer Sciences Corporation, Columbia, MD*

1998-2000

Played significant role in the evaluation of commercial products for compliance with ISO 15408-1 (*Common Criteria for Information Technology Security Evaluation*). Conducted information security risk assessments for federal and state government agencies, focusing on architectural, physical, and personnel security.

Consultant*KPMG Peat Marwick LLP, Washington, DC*

1997-1998

Conducted information security risk assessment for federal and state government agencies, focusing on architectural, physical, and personnel security. Served as project manager for 30% of engagements.

Captain(P), Military Intelligence*United States Army, Various Locations*

1987-1998

All-source intelligence officer. Developed, implemented, and managed the physical, computer, personnel, document, information, and crime prevention programs in 75% of assignments (both in peacetime and during Operation Desert Storm). As a counterintelligence detachment commander in Western Europe, supervised the successful execution of over 3000 personnel security investigations in a two-year period. Planned and conducted risk assessments for 5 US and NATO military installations in 4 countries.

EDUCATION & CERTIFICATIONS

M.S., Information Assurance (cum laude)

Norwich University, Montpelier, VT

June 2007

B.S., Computer Sciences

US Military Academy, West Point, NY

May 1987

Certified Information Systems Manager (CISM)

ISACA

2004-Present

Certified Information Systems Security Professional (CISSP)

(ISC)2, Shrewsbury, MA

1999-Present

ADDITIONAL INFORMATION**Top Secret Security Clearance***US Department of Defense*

1987-1998, 2009-2012

Member, CISO Advisory Council*International Systems Security Association*

2009-2014

Security Fellow*International Systems Security Association*

2015-Present

Top 25 Finalist, CISO Breakaway Leaders Award*Evanta*

2013