Andrew R. Reese

Kansas City, Missouri Area
Phone: 717-395-3063
Email: Andy.Reese@ReeseWeb.Com

CISSP, CISM, CRISC, CGEIT, CPP, ITIL

Security & Compliance Practice Leader

Summary

Highly respected professional services practice leader delivering subject matter expertise with extensive hands-on experience assessing, designing, implementing, testing, and managing security policies, processes, procedures, and controls for organizations of all sizes and vertical markets. Talent areas include: Security Strategy, Cybersecurity Thought Leader, "C" Suite and Board of Director Communication, Complex Security Topic Translation to Business Audiences, Enterprise Information Security, Emerging Security Threats, Consensus Builder, Executive Collaboration, Enterprise IT Risk Management, Global Regulatory Compliance, Security Management Program Development, Business Unit Collaboration, Business Analysis, Security Awareness, Security Policies / Security Procedures, Budgeting, Data Privacy, Gap Analysis, Incident Response, Business Continuity and Disaster Recovery Planning, and Data Governance.

Education

- Bachelor of Computer Science, American Institute for Computer Science (GPA 4.0)

Prominent Certifications

- **CISSP** #25685 – (ISC)^2 Certified Information Systems Security Professional
- **CISM** #0300317 – ISACA Certified Information Security Manager
- **CRISC** #1000038 – ISACA Certified in Risk and Information System Controls
- **CGEIT** #0800964 – ISACA Certified in Governance of Enterprise Information Technology
- **CPP** #17243 – ASIS International Certified Protection Professional
- **ITIL v3** #10060937 – Certified Information Technology Infrastructure Library Foundation
- Years of Security Vendor Product Certifications and Hands-On Experience

Tested Skills By Prominent Certifications

Access Management
Asset Security
Business Continuity
Business Principles and Practices
Communications Security
Computer Security
Disaster Recovery
Enterprise IT Governance
Identity Management
Information Risk Compliance
Information Security
Information Security Management
Information Technology
IT Benefits Realization
IT Control Maintenance
IT Governance
IT Governance Framework
IT Governance Principles
IT Resource Optimization
IT Risk Assessment
IT Risk Evaluation
IT Risk Identification
IT Risk Management
IT Risk Monitoring
IT Risk Optimization
IT Systems Control Design
IT Systems Control Implementation
IT Systems Control Monitoring
IT Security
IT Security Incident Manager
IT Security Program Manager
Network Security
Penetration Testing
Personnel Security
Physical Security
Professional Services
Project Management
Risk Management
Security
Security Assessment
Security Audits
Security Engineering
Security Management
Security Operations
Security Principles and Practices
Security Testing
Software Development Security
Strategic IT Management
Vulnerability Assessment

Professional Experience

CompuCom Systems, Inc. 2005 to Present

A $10.8B global service company that supports 5.15-million users, 6.4-million devices, with 11-thousand employees, 100-thousand certifications, 6-thousand technicians. We resolve more than 90% of service desk calls on the first contact. 70% if IT services revenue is from recurring annuity clients. 97% of our revenue comes from repeat clients. Who are our clients: 6 of the top 10 Fortune 500 companies, 7 of the top 10 retailers in North America, 6 of the top 10 financial services firms in North America.

Security & Compliance Practice Leader January 2005 to Present
Managing Principal May 2016 to Present
Principal Consultant January 2005 to May 2016

Security Strategy: See and understand security concerns others may not see. Translate complex cyber security topics to business audiences. Helped hundreds of companies successfully align their security strategy, people, processes, technology and culture. Extensive experience with security technology implementations that decrease the time to detect indicators of compromise using infrastructure and endpoint security instrumentation and decrease the time to respond to events with artificial intelligence and automation.

Cybersecurity Thought Leader: Personally led hundreds of security workshops, providing needed security education and knowledge transfer. Helped numerous organizations improve the maturity and quality of their Security Management processes and controls, security.

"C" Suite and Board of Director Communication: Well-versed in many communication tools. Skilled in keeping the message short and to the point. Advised various Executive Committees and Board of Directors on risk issues that are related to information security and recommended actions in support of their organization's wider risk management program.

Complex Security Topic Translation to Business Audiences: Led professional security practices performing security-consulting engagements across multiple vertical markets. Honed skills in translating complex cyber security topics to business audiences.

Enterprise Information Security: Certified ISO/IEC-27001 Lead Auditor of security, with extensive knowledge of industry frameworks and architectures, standards, benchmarks, guidelines and best practices. Significant professional consulting experience working with organizations from small to medium size businesses (SMB), to large global enterprise companies.

Emerging Security Threats: Active board member of the local FBI Infragard chapter for protecting our nation's critical infrastructure. Maintain frequent contact with security industry leaders, numerous early warning systems, as well as receive alerts and notifications of critical infrastructure threats. Lead global threat intelligence networks, databases and threat feeds.

Consensus Builder: Assisted organizations to build and document consensus, such as, but not limited to: interactive onsite or remote consensus building workshops, information security management forums or steering committees, information security management system (ISMS) benchmarks and more.

Executive Collaboration: Worked with corporate officers, legal counsel, human resources, and facilities / physical security relative to difficult security and privacy issues. Worked with executive teams to inform them of current and future risks, understand their perspectives on organizational risk, risk decisions and priorities, compliance requirements, security budget and more.

Enterprise IT Risk Management: Developed, implemented and monitored a comprehensive enterprise information security and risk management program. The program included the process of planning, organizing, leading and controlling risk management activities, defining and documenting legal, regulatory and contractual security requirements, performing business impact and risk assessments, applying methods for limiting and managing different levels of risks tolerance and exposure.

Global Regulatory Compliance: Well-versed in security control harmonization and the tools from the Unified Compliance Framework. Assisted clients to harmonize their security processes and controls, implemented scoped statement of applicability documents, and more.

Security Management Program Development: Implemented and improved the lifecycle of client's information security management system/program (ISMS). Developed tools and methodologies used during professional engagements for measuring and benchmarking the maturity of security processes and controls across global organizations. Performed many professional ISMS benchmark engagements for large global enterprise organizations. Strategically road mapped short, medium and long-term plans, level of work effort, resource requirements and costing, and then successfully executed to plan, on time and on budget.

Business Unit Collaboration: Experienced in articulating security requirements and soliciting business unit collaboration on global, regional and local policies, standards, benchmarks, guidelines, processes and procedures. Well versed on how to document roles and responsibilities across a global organization; such as, how to identify who is accountable, responsible, consulted, informed, sponsors, and supports various security controls, based upon well-defined scopes and statements of applicability, memorandums of understanding, operational level agreements, service level agreements and under pinning contracts.

Business Analysis: Developed, provided knowledge transfer and directed technical teams of numerous organizations in how to implement continuous process and operational improvements in their security management systems.

Security Awareness: Worked with human resources and legal teams to ensure compliance with legal and regulatory requirements, as well as, maintain end-user security awareness and understanding via customized communication tools, learning management system training systems, strategically positioned posters and plaques, security tip newsletters and more.

Security Policies / Security Procedures: Designed security policy architecture and flow. Formulated and wrote policy content, compliance mapping and linking, reviews and approvals, access and permission controls. Created security processes and procedures with decision points, inputs, outputs, documentation requirements and compliance mapping and linking. Used the Unified Compliance Framework.

Budgeting: Established resource staffing requirements and project budgets on a weekly basis for service engagements. Worked with clients across North America to provide security solutions to solve their problems in a cost effective manner. Delivered services and implemented technologies per the terms and budget of contractual agreements.

Data Privacy: Leveraged cryptography technologies for data at rest and in motion; the application of masking, controlling access to, minimize exposure by devaluing the data through encryption and tokenization and more.

Gap Analysis: Performed gap assessments including: legal, regulatory, and contractual requirements assessments; business impact and risks assessments; network vulnerability, application static binary and dynamic secure coding practices, and manual penetration test assessments; information security management system (process and control) maturity benchmarking assessments; compliance gap assessments; configuration benchmark assessments; and more.

Incident Response: Experienced with Security Information Event Management (SIEM) technologies. Performed forensic analysis, recovery and reviews of lessons learned. Skilled in instrumenting the network infrastructure and endpoint systems with technology that reduces the time to detect indicators of compromise, gather evidence, and to respond to incidents. Strategically applied artificial intelligence and automation to minimize impacts.

Business Continuity and Disaster Recovery Planning: Helped numerous organizations with strategic vision and evolution by developing and designing high availability, capacity, business continuity and disaster recovery plans for their critical IT assets. Orchestrated periodic testing and demonstrated recovery using various scenarios.

Data Governance: Assisted numerous clients with creating well-written policies, highlighting data sensitivity for end-user awareness, applying appropriate processes and technologies for inventorying what data is stored where, applying the right data classification and meta-tagging, sensitivity handling while in transit and at rest, data loss prevention, reduction of sensitive data sprawl, retention requirements, permission and access management, authenticity, non-repudiation, chain of custody, data integrity, much more.

DynTek, Inc. **March 2003 to October 2004**
National Director of Security Consulting and Virtual CxO

Reese Web Security, Inc. **January 2003 to December 2004**
Vice President, Florida Licensed Private Investigation Company (Co-Owner)

AimNet Solutions Inc. **May 2000 to December 2002**
Vice President, Chief Security Officer, and Information Security Practice Leader (Co-Owner)

Reese Web, Inc. **August 1995 to May 2000**
Chief Executive Officer & President (Owner) – National Security Company

The Waldec Group **December 1994 to August 1995**
Director of Network and Advanced Network Services

Nielsen Media Research **June 1993 to December 1994**
LAN Coordinator

McDonnell Douglas **October 1992 to June 1993**
Senior Engineer - Technology

Halifax Corporation **June 1986 to October 1992**
Field Service Representative to European Regional Manager

Eaton Corporation **January 1985 to June 1986**
Associate Field Engineer

Enfield's 3M Business Products **April 1984 to January 1985**
Customer Service Representative

U.S. Navy **January 1978 to January 1984**
USS George Bancroft SSBN 643 Blue Crew
Fire Control Technician Ballistic Missile First Class E-6 (Submarine Service) - FTB1(SS)

Industry Involvement

- InfraGard National Members Alliance (INMA) - North Central Regional Deputy Representative
- InfraGard Kansas City Members Alliance (IMA) - Member of the Board of Directors
- InfraGard Kansas City Members Alliance (IMA) – Webmaster (InfraGard-KC.Org)
- Wounded Warrior Project – Mentor to U. S. Military Veterans
- Safe & Secure Online by (ISC)^2 – Authorized Volunteer
- InfraGard, ASIS International, ISACA, (ISC)^2, and OCEG – Active Member
- Years of Security Industry Articles and Security Tip Newsletters
- Years of Technical Advisory Board Experience for Many Leading Security Vendors
- Security Clearance: 1978-1996 TS/SBI (SCI)

Special Note: InfraGard Kansas City Members Alliance (IMA) is a non-profit organization serving as a public-private partnership among U.S. businesses, individuals involved in the protection and resilience of U.S. critical infrastructures, and the Federal Bureau of Investigation.