Andrew Shumate

Hampton, VA • (757)744-9076 • resume@andrewshumate.com • linkedin.com/in/andrewshumate

Focus on security first as a business principle, and all of your compliance needs will come naturally.

I help organizations build security programs that protect their business while enabling growth.

With more than 30 years of experience spanning enterprise security architecture, cybersecurity consulting, governance, risk and compliance, and military cyber operations, I've partnered with organizations of all sizes—from emerging businesses to global enterprises—to strengthen their security posture and navigate complex regulatory environments.

Throughout my career, I've designed enterprise security architectures, led security assessments, developed information security programs, and advised executive leadership on cyber risk, governance, and strategic initiatives. My experience includes ISO 27001, NIST, FedRAMP, HIPAA, PCI, SOC, CMMC, and other leading security frameworks, helping organizations translate technical requirements into practical business solutions.

I'm passionate about mentoring security professionals, developing innovative security solutions, and helping organizations build resilient security programs that align with business objectives.

WORK EXPERIENCE

Pirate and Mermaid Vacations — 11/2015 - Present
Co-Owner and President

- Own end-to-end corporate compliance for a multi-state small business: annual and foreign-entity corporate filings (VA, FL, CA, WA), business licensing and Seller of Travel registration, corporate income tax and BOI filings under the Corporate Transparency Act, USPTO trademark registration and maintenance, and insurance compliance — in addition to AP/AR, bookkeeping, and IT functions.

CDW — 05/2017 - 07/2026
Principal Global Enterprise Security Architect

- Led development of secure solution architectures spanning business, application, data, and infrastructure domains across a global, multi-business-unit enterprise, translating security requirements into terms system owners and business stakeholders could act on.
- Began development of enterprise-wide information security baselines to unify and standardize controls across CDW's global business units and entities.
- Created and maintained security patterns and solution blueprints in partnership with fellow architects, ensuring designs adhered to security standards before reaching engineering and development teams.
- Provided decision support and risk-based recommendations directly to technology, business, and program leadership on target-state architecture investments.

Managing Consultant, Information Security

- As a trusted advisor, assessed gaps against ISO 27001, FedRAMP, NIST, HIPAA, PCI, SOC 2, and CMMC and built GRC programs, risk registers, and information security policy sets from the ground up for a broad portfolio of clients.
- Founded and scaled CDW's CMMC assessment practice, including the firm's registration as a Registered Provider Organization (RPO) — taking a new service line from concept to delivery capability.
- Designed a new information security gap-assessment offering built on the NIST Cybersecurity Framework, expanding CDW's addressable services.

- Served as technical estimator for pre-sales solution architects on bespoke security assessment engagements, scoping level-of-effort for novel or client-specific regulatory frameworks; identified recurring client demand for an emerging framework (Texas SB 820) and built it into a standard, repeatable service offering.
- Strengthened clients' security incident response programs through designing and leading innovative tabletop exercises, fostering collaboration and strategic thinking among stakeholders.
- Presented aggregated risk findings from a 12-hospital healthcare conglomerate assessment directly to the client's board of directors; anonymized individual facility results (using cryptonyms) to preserve candor and drive accountability without singling out stakeholders in a board setting — one facility voluntarily self-identified and took ownership of its findings during the meeting.
- Regularly briefed customer C-level executives on assessment findings, risk posture, and remediation priorities in both technical and business terms.
- Advised a client on GDPR compliance and helped develop the resulting data-handling policy; built plain-language teaching frameworks to translate the legal distinction between marketing/behavioral data use and protected transactional data for non-technical executive audiences.
- Advised clients on emerging AI/ML governance risk, including data-leakage exposure from AI agent access to sensitive systems; designed incident-response tabletop exercises simulating misguided or uncontrolled AI use.
- Advised clients on structuring third-party/vendor risk programs and fielded early questions on AI/ML governance as those risks began surfacing in client environments.
- Served in a staff-augmentation SOC Manager role for a client, including interviewing and helping select the client's permanent SOC Manager.
- Partnered with sellers to architect custom security solutions for customer needs with no existing service-offering fit.

Pivot Point Security **07/2014 - 05/2017**
Senior Information Security Consultant and Auditor

- Built and assessed Information Security Management Systems against ISO 27001, FedRAMP, NIST/FISMA, and ISO 22301, and against regulatory frameworks including HIPAA, PCI, PII, NERC, and SOX.
- Performed ISMS audits for 13 clients, each achieving ISO 27001 certification, and guided clients end-to-end through FedRAMP Certification and Accreditation, authoring System Security Plans, policies, and compliance artifacts spanning regional businesses to top-100 national law firms.

U.S. Navy **01/1994 - 07/2014**
Computer Network Defense Analyst

- Planned and led Computer Network Defense assessments of Navy networks worldwide across 90+ engagements, and evaluated and helped develop the tools, techniques, and procedures used by Navy Blue and Red Teams.
- Delivered written risk analysis and security-trend reporting that senior Navy leadership used to set network policy.
- Briefed ship commanding officers (O-5/O-6) on network security assessment findings as a junior enlisted analyst; sought out directly by flag officers (Admiral-level) for cybersecurity explanation and context outside the standard chain of command.
- Revitalized the Blue Team's Computer Network Defense training program and consolidated training/assessment teams, saving the Navy over $250,000 annually while improving operator qualification standards.

Information Assurance Manager

- Led a team of three and directed an Integrated Process Team that consolidated seven sites' IT and Information Assurance policies into a single command.
- Owned the command information security program end-to-end and tracked Information Assurance/PII awareness training compliance for 2,543 personnel across seven geographically dispersed sites, alongside 430+ managed assets.
- Ensured that all physical and personnel security requirements for legacy and Navy Marine Corps Intranet (NMCI) were met in accordance with governing policies.

- Served as command point of contact for NCIS, CTF-CND, and NAVCIRT on all security incidents.

Aviation Maintenance Supervisor (Manager)

- Managed the maintenance operations of 16–24 personnel, including tool/test-equipment control, classified information handling, and personnel management.

Aviation Electronics Technician

- Responsible for maintenance of the AN/APG-65/73 Fire Control RADAR system and all associated computer test equipment in accordance with published maintenance and quality assurance practices.
- Collaborated with cross-functional teams to participate in ship-wide emergency response drills, working to reduce response time and improving overall crisis management effectiveness.

EDUCATION

Master of Business Administration
University of Arizona Global Campus

Master of Science, Cybersecurity Policy
University of Maryland University College

Master of Science, Information Technology: Information Assurance
University of Maryland University College

Master Certificate, Information Systems and Operations
Naval Postgraduate School

Bachelor of Science, Computer Networking
Strayer University

CERTIFICATIONS

CISA	04/2015
PECB Certified ISO/IEC 27001 Lead Implementer	04/2015
CISSP	07/2014
Core Impact Certified Professional	08/2012
CompTIA Security+	10/2008
CompTIA Linux+	06/2007
Microsoft Certified Systems Engineer (Windows 2000)	10/2003

VOLUNTEERING & LEADERSHIP

BSidesDC
CryptKids cryptography and capture the flag competitions facilitator

Developed and facilitated the BSidesDC CryptKids cryptography and capture the flag competitions, which are both designed to educate children ages 7 – 17 in codes, ciphers, and computer security fundamentals.

DC757 DEF CON group
Founding member

CONFERENCE PRESENTATIONS

Cryptkids Crypto Lab and CTF Primer 10/2017
BSidesDC
Durring this hands on workshop, attendees will walk through the CryptKids Crypto Challenge and CTF to gain the understanding and confidence to participate in conference capture the flag competitions.

Building the Poison Apple Pie

10/2016

BSidesDC

Everyone loves the Raspberry Pi, it's cheap, relatively powerful for its size, portable, and versatile. After being inspired by the idea of a discrete system for wireless assessments, the idea for the Poison Apple Pi was born; designed to be an inexpensive, portable, modular discrete platform for security testing the Poison Apple leverages many available code and tools to develop a testing platform that can be carried in a backpack, or deposited and retrieved later. This talk will cover the hardware and software used, configuration, possible use cases, and future potential.

Cyber War Stories

03/2015

CarolinaCon 11

Have you ever been involved in an incident response and had to deal with tool sprawl where no one can account for system management utilities?

To counter this problem, a 'Tool Control Program' could be put in place at the enterprise level. This program is simply the centralization, standardization and documentation of tools and utilities used. Though this process any dual use tool that is found on the network can easily be identified as either a legitimate tool used for network operations or as an indicator that an intruder has copied it over for nefarious purposes.