https://jdavis.tech/ **Jay Davis, CISM** www.linkedin.com/in/jay-davis
jay@jdavis.tech

Cyber Security Specialist

Progressive attitude, outstanding ethics and unparalleled enthusiasm MEET your Poster Child!

A technology compliance leader and mentor with over 20+ years of systems and cybersecurity experience in cloud and physical environments. Expertise in leading Governance, Risk and Compliance (GRC) teams for enterprise solutions through enterprise information risk management, risk assessments, policy, standards and application assessments, vulnerability and remediation, Identity Access Management (IAM) and IT Auditing.

In-depth knowledge of multiple security and regulatory standards (NIST, HIPAA, SOC, SOX, ISO, PCI-DSS, GDPR, COBIT, OWASP, ITIL, etc.).

Currently in my final year of my Bachelor of Science Degree in Cybersecurity and Information Assurance. Maintained a DoD Security Clearance from 01/2002 to 03/2017 when the clearance was archived for inactivity.

Key Career Accomplishments

- Achieving a PCI-DSS Attestation of Compliance (AOC) by leading the teams responsible for resolving, remediating, mitigating, and/or establishing compensating controls of data management for over 7,500 pentest vulnerabilities, within a 19-day deadline.
- Leading a bi-annual internal audit process to establish the Authority to Operate (ATO), consistently for a three-year period. Led teams to provide evidence for over 100,000 individual configuration settings, within short deadlines. Based on compliance to the NIST 800-53 Configuration Management controls as defined by multiple Secure Technical Implementation Guide's (STIG's).
- Reduced vulnerabilities from over 60,000 non-compliant NIST 800-53 configuration findings to zero. Achieving operational compliance for an enterprise structure consisting of four locations with over 11,000 employees serving 21.5 million people.
- Managed, led, and mentored 16-member Service Desk team, providing multiple tier level technical production support in a complex war zone environment.

Key Processes

Change Management, *Project Management*, Incident Management, *Endpoint Protection*, Vulnerability and Threat Assessments, *Risk Assessments*, Remediation and Mitigation, *Information Security*, Security Documentation, *Emotional Intelligence*, Mentorship / Leadership / Negotiation Skills and *Information Management*.

Certifications

Certified Information Security Manager (CISM) *(Certification # 1840465)*

Information Technology Infrastructure Library (ITIL v4) *(Certification # GR67118297JD)*

Certified Incident Handler (ECIH) *(Certification #ECC7134958062)*

Certificate of Cloud Security Knowledge (CCSK) *(Code: 5gcoMUtyn7Zc4oe7zAaRVwiQ)*

Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 *(Certification # F018-5583)*

Certified Identity and Access Manager (CIAM) *(Certification # 4239)*

Certified Access Management Specialist (CAMS) *(Certification # 4238)*

VMware Certified Professional (VCP5-DCV) *(Code: 11374564-91D1-97DC9ED1B49B)*

CompTIA Security +; A +; Network +

Professional Experience

Bank of America

Senior Global Security Specialist – Policy Assessment, Dallas, TX *10/2019 - present*

Member of the GIS – Policy Assessment Team specializing in application policy adherence for financial services.

- Executing Security Assessments for financial institution's applications incorporating Confidentiality, Integrity and Availability (CIA) standards.
- Assisting risk mitigation involving applications for business performance, legal and security compliance for the production and testing environments.
- Using financial institution methodology which incorporate PCI-DSS, NIST, SOX, SOC, GDPR, FFIEC and ISO standards and regulations towards CIA assessment posture.
- Collaborating with application managers and their delegates, Quality Assurance (QA) and Configuration Management (CM) teams to ensure required application posture is met for GIS, CSTAR and FFIEC assessments.

Alorica

Global Cyber Security Analyst, Dallas, TX 11/2018 – 03/2019

Leadership of the Information Security Team specializing in architecture and Governance, Risk and Compliance. Project technical / team lead for the PCI-DSS re-certification of the AOC/ROC.

- Resolved, remediated, mitigated, and established compensating controls for 7,500+ Pen Test vulnerabilities including root cause analysis, intrusion detection and architectures allowing the organization to regain their AOC (Attestation of Compliance) through a clean Penetration Test and strong negotiation skills.
- Developed SOC 2 Type 1 (procedures and controls) and Type 2 (proof of procedures and controls) compliance reports for data center networks, firewalls, routers, security systems and system configuration best practices required by American Express resulting in cessation of imposed fines.
- Led the corporate posture (with one other engineer) for Identity Access Management (IAM), Mobile Device Management (MDM) and Single Sign-On (SSO) solutions to be fulfilled through third-party vendor contracts.
- Influenced the strategy for the Security Operation Center (SOC) to categorize and prioritize findings, implement necessary regulatory requirements and security policies and procedures.
- Forged long-term strategic networking relationships with the teams responsible for remediation, negotiation and the managerial, marketing materials to budget time and resources for Infosec.

Blue Cross Blue Shield of SC

Sr. IS CyberSecurity Engineer, Dallas, TX 03/2015 – 06/2018

Creator, Leader, and Motivator of the Operational Systems Compliance (OSC) Team effectively training and mentoring OSC staff in a strategic direction for information assurance practices. In accordance with corporate FCRA, GRC, HIPAA and DISA STIG standards meeting NIST and organizational RMF requirements.

- Reduced 60,000+ non-compliant findings to zero through proactively influencing a strategic direction of control activities with decision making innovation in data management for Windows OS, virtual environments, group policy and active directory.
- Encouraged internal collaboration teams to focus on vulnerability assessments, risk assessments, issues, creative solutions and organized remediation or mitigation techniques thus reducing impact and achieving 40% reduction in total organizational vulnerabilities.
- Created policy development and security documentation for organizational compliance, allowing for enterprise risk management implementation. Created Business Risk Justification's, Policies and POAMs, system security plans, security controls traceability matrices, and security requirements to support the Authority to Operate (ATO) Regulatory Examination.

General Dynamics Information Technology - PACOM
Sr. System Engineer / Administrator, Oahu, HI 07/2012 – 03/2015

Created, provisioned, and maintained enterprise-level servers and workstations for multiple world- wide classified networks for DoD in the Pacific Command achieving and maintaining NIST compliance.

- Created and maintained anti-virus and backup systems for organizational integrity.

General Dynamics Information Technology - USACE
Sr. System Engineer / Administrator - IANO, Kabul, Afghanistan 02/2011 – 06/2012

Served as Information Assurance Security Officer (IASO), Service Desk Manager and Sr. Systems Engineer / Administrator in virtual and physical enterprise environments for the Northern Afghanistan Region of USACE.

Manager, leader and mentor of the 16-member collaborative enterprise service technologists' team, providing systems support for Tier I - IV incident and issues.

Education

Currently completing my final year for the WGU B.S. in Cybersecurity and Information Assurance. Preparing for the CISSP certification. Awaiting certification for Certified Cloud Security Professional (CCSP) and the Certified Encryption Specialist (ECES).

System Security Assessments / Hardening Tools:

Nessus, Tripwire, Qualys, CVSS, STIG Viewer, Active Directory/Group Policy, Symantec Endpoint Protection/ Backup Exec in addition to the SANS 20 Critical Security Controls