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

GRC | Risk Assurance

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 data control experience in cloud and physical environments. Self-Motivated in leading Governance, Risk and Compliance (GRC) teams for enterprise solutions and data loss prevention.

Guiding enterprise data control risk management strategies for emerging and existing risks, risk and control assessments, vulnerability and remediation management, Identity Access Management (IAM) and internal IT auditing. Outgoing and energetic with collaborative relationship building towards teams' cohesion.

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

- Currently in my final year of my Bachelor of Science Degree in Cybersecurity and Information Assurance.

Maintained a DoD Security Clearance for 15 years.

Key Career Accomplishments

Conduct stakeholder, business leaders, executive, third party, and technical staff project and progress meetings. Relationship and confidence building meetings with disparate remediation / mitigation staff and leadership.

Achieved a PCI-DSS Attestation of Compliance (AOC) by leading the teams responsible for resolving controls for data management in over 7,500 pentest vulnerabilities, within a short deadline.

- Leading teams for bi-annual internal audits to establish the Authority to Operate (ATO).
    - Delivering a consistent, collaborative, innovative high-quality solution, while leading cross-functional teams to provide evidence for over 100,000 individual configuration settings.
    - In 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.

Created a reporting process using Microsoft Office Excel, PowerPoint, Visio, Outlook and Word to facilitate technical and executive staff understanding.

- Managed, led, and mentored 16-member Service Desk team, providing 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*, Facilitation Skills, *Emotional Intelligence*, Mentorship / Leadership / Negotiation Skills and *Data Loss Prevention*.

Certifications

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

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

Certified Data Privacy Solutions Engineer (CDPSE) *(Certification #2113620)*

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)*

Professional Experience

Bank of America

Sr Global Security Specialist – Policy Adherence Assessments, Dallas, TX 10/2019 - present

Senior Member of the GCOR – Application Policy Assessment Team specializing in application policy adherence.

- Executing Application Security Assessments for financial institution's applications incorporating Confidentiality, Integrity and Availability (CIA) policies and standards.
    - Using financial institution methodology which incorporate regulatory and ISO standards towards CIA assessment posture.
- Provide leadership and guidance for teams in their assessments for application controls
    - Perform assessment Quality Assurance (QA) reviews.
    - Write findings/observations for failed controls.
- Review corporate and industry policies and their updates for applicability to the bank environment
    - Recommend corresponding methodology and control adjustments.
- Assisting risk mitigation involving applications for data control, business performance, third party risk, legal and security compliance for organizational applications.
- Collaborating with application managers and their delegates, Quality Assurance (QA) and Configuration Management (CM) teams to ensure required application posture 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 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 and 2 audit reports and compliance reports for data center, security system configuration best practices required by American Express resulting in cessation of imposed fines.
- Led the corporate posture for Identity Access Management (IAM), Mobile Device Management (MDM) and Single Sign-On (SSO) solutions to be fulfilled through third-party vendor.
- Forged long-term strategic networking relationships with interpersonal communication skills for the teams responsible for remediation, negotiation and management 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 team in a strategic direction for information assurance practices. In accordance with corporate FCRA, HIPAA and DISA standards, meeting NIST and RMF requirements.

- Reduced 60,000+ non-compliant findings to zero through audit planning and working with team leads and 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 and risk assessments with issue management. Point of Contact for creative solutions and organized remediation or mitigation techniques thus reducing impact and achieving 40% reduction in total organizational vulnerabilities.

- Writing 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 server and workstation images for deployment.
- Created network and server virtual environment with VMware.
- Created and maintained anti-virus and backup systems for organizational integrity.

General Dynamics Information Technology - USACE
Sr. System Engineer / Administrator – IASO, 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 the United States Army Corps of Engineers (USACE).

- Manager, leader and mentor of the 16-member collaborative enterprise service technologists' team, providing systems support for Tier I - IV incident and issues.
- Creator of Backup/Archive solution for the Northern and Southern Afghanistan Regions of USACE.

Lockheed Martin – Meganoc, DoJ
Sr. System Administrator, Level IV, Washington, DC 10/2010 – 02/2011

Served as Systems Admin Manager for the team to upgrade NIST 800-53 revision 3 to revision 4.

- Upgrade backup/archiving solution allowing for deduplication improvements.
- Upgrade and implement BCDR program for new site relocation.

Education

Currently completing my final year for the WGU B.S. in Cybersecurity and Information Assurance.
Coursework includes: Network, Web and Cloud Security; Data management; Digital Forensics; Risk management; Cryptography; Cyber defense; Penetration testing; Scripting and programming; Web development, etc.
Preparing for the CISSP certification. Scheduled for certification of Certified Cloud Security Professional (CCSP).

- Certified Incident Handler (ECIH) *(Certification #ECC7134958062)*
- Certified Access Management Specialist (CAMS) *(Certification # 4238)*
- VMware Certified Professional (VCP5-DCV) *(Code: 11374564-91D1-97DC9ED1B49B)*
- CompTIA Security +; A +; Network +

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.