https://jdavis.tech/

Jay Davis

www.linkedin.com/in/jay-davis

Jay@jdavis.tech | JayR98Davis@Hotmail.com

Governance, Risk and Compliance

A technology compliance leader and mentor with over 30 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. Successfully driving compliance programs from conception to fruition.

Guiding enterprise risk management data control strategies for emerging and existing risks, application risk and control assessments, gap analysis, vulnerability and remediation management, and Identity Access Management (IAM). In-depth knowledge of multiple regulatory standards (NIST, HIPAA, SOC, ISO, PCI-DSS, GDPR, ITIL, etc.).

- Providing Cloud Guidance for IaaS, PaaS and SaaS environments for organizational structure and operations.
  - Using the Cloud Security Alliance (CSA) standards for Cloud Controls Matrix and the STAR registry
- Currently in my final year of my Bachelor of Science Degree in Cybersecurity and Information Assurance.

Maintained a DoD Secret, Top Secret and TS/SCI Secret Security Clearance for 15 years.

Key Career Accomplishments

Manager for a 16-member Service Desk team, providing technical production support in a complex war zone environment in Northern Afghanistan for the US Army Corps of Engineers (USACE).

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

- Conduct Bank Applications Control Gap Assessments encompassing User Accounts, User Access, Log Details, Log Monitoring, Report Accounts, Confidential Data, and Authentication Services.
  - Creation and maintenance of Question and Evidence Guides and Pre-Work Guide documentation.
- Modify / Publish Bank policies and standards to meet annual upgrades for the Policy Adherence Assessment group:
  - Monitoring, Response and Forensic (MRF); Cryptography (KEY); Data Protection (DAP); Identity and Access Management (IAM); Application and Security (APS); Infrastructure (INF)

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

- 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 with the NIST 800-xx 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.

Key Processes

Change Management, *Project Management*, Incident Management, *Endpoint Protection*, Vulnerability and Threat Assessments, *Risk Assessments*, Control Gap Assessment with Remediation and Mitigation, *Information Security*, Facilitation Skills, *Emotional Intelligence*, Mentorship / Leadership / Negotiation Skills and *Data Loss Prevention*.

Certifications *(additional certifications on the last page)*

Certified Information Security Manager (CISM) *(Certification # 1840465)*
Information Technology Infrastructure Library (ITIL v4) *(Certification # GR67118297JD)*
Certified Data Privacy Solutions Engineer (CDPSE) *(Certification #2113620)*

Professional Experience

Bank of America

VP, Global Risk Management Dallas, TX 10/2019 - present

Senior Member of the GIS – Application Risk Assessment Team for application policy adherence with a team of 8 assessors.

- Executing Application Security Risk Assessments and GAP analysis for financial institution's 2nd line of defense for applications incorporating Confidentiality, Integrity and Availability (CIA) policies and standards.
  - Using bank methodology incorporating policies and standards posture for: *Identity Access Management;* Logging and Monitoring; *Data Access Protection;* User Access Management; *Authentication Services;* Confidentiality Data Control; and *Privileged Access Review.*
- Provide leadership and guidance for teams in their risk and third-party assessments for application controls
  - Perform assessment Quality Assurance (QA) reviews.
  - Write findings/observations for failed controls.
- Review policies / standards updates for applicability to the Policy Adherence Assessment group
  - 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 Risk Security Team specializing in GRC. Project lead for the PCI-DSS re-certification

- Resolved, remediated, mitigated compensating controls for 7,500+ Pen Test vulnerabilities including root cause analysis, intrusion detection allowing the organization to regaintheir AOC through a clean Pen Test.
  - AIC (Auditor in Charge) for SOC 2 type 1 and 2 audit reports and compliance reports for data center, security system configuration required by American Express resulting in cessation of imposed fines.
- Led the corporate posture for Identity Access Management (IAM), MobileDevice Management (MDM) and Single Sign-On (SSO) solutions to be fulfilled through a third-party vendor.

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 towards a strategic direction of control and innovation in data management for NIST configuration controls.
- Creation and managed internal collaboration teams to focus on vulnerability and risk assessments management. Solutions and Issue Management techniques achieving 40% reduction in total organizational vulnerabilities.
- Writing policy development and security documentation for organizational compliance, allowing forenterprise 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.
- Established network and server virtual environment with VMware.
- Crafted 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 incidents 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. Degree in Cybersecurity and Information Assurance.

Certifications: *(Continued from first page)*

- Certificate of Cloud Security Knowledge (CCSK) *(Code: 5gcoMUtyn7Zc4oe7zAaRVwiQ)*
- Certified Identity and Access Manager (CIAM) *(Certification # 4239)*
- Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 *(Certification # F018-5583)*
- 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.