Jay Davis, *CISM, CCSKv4, MCSA*

North Dallas, TX 75044

jay49davis@hotmail.com (703) 915-8659 www.linkedin.com/in/Jay-Davis

CYBER SECURITY ENGINEER | LEADER | GOVERNANCE - RISK – COMPLIANCE

Leveraging Business Values into Strategic GRC Solutions

A tenacious technology leader and engineer with extensive comprehensive *cloud*, *systems* and *security* experience with a demonstrated ability to provide *Governance, Risk and Compliance (GRC)* for *Enterprise Solutions, forge strategic business alliances* and *continuous educational / knowledge improvement*. Development of *cyber security requirements*, document / review *security policies* and *procedures*, assess *security services* and *technology*, ensuring *Enterprise Information security risks* are identified, reported, and tracked through their life cycle and properly dispositioned via *elimination*, *acceptance*, *transfer*, or *reduction*.

Core Competencies

An Organizational GRC and Security Motivating Force!

- ✦ Cloud Governance, Auditing & Compliance
- ✦ Risk and Vulnerability Assessments & Remediation
- ✦ Identity Access Management
- ✦ Troubleshooting & Remediation Coordination
- ✦ Information Security Documentation Specialist
- ✦ Information Assurance Training
- ✦ Continuous Educational Pursuits
- ✦ Cyber Security Standards: *ISO 270xx, NIST 800-xx, FEDRAMP, SOC I, SOC II, SOX, PCI DSS*
- Enterprise & Information Risk Management ✦
- Policies / Standards Creation and Enforcement ✦
- Strategic Relationship Building ✦
- Auditing Deliverables ✦
- Windows Level IV Engineering ✦
- Virtualization ✦
- Currency in GRC Topics / Techniques ✦

Career Progression

Sr. IS Security Engineer *03 / 2015 – 06 / 2018*

TM Floyd & Company | Blue Cross Blue Shield of SC (Dallas, TX)

Leader and Creator of the Operational Systems Compliance *(OSC)* Team – effectively training and mentoring OSC staff to enable effective Information Assurance *(IA)* practices – in accordance with *DISA STIGs, NIST 800-53, ISO 9001:2015* and organizational Risk Management Framework *(RMF)* requirements.

- Encouraging daily team operations for vulnerability assessments and remediation/mitigation techniques across multiple platforms for the application, middleware and infrastructure owners, achieving 40% reduction in non-compliant vulnerabilities.
- Create security documentation for the implementation of Organizational Compliance standards: Policies; Standards; Guidelines and Work Instructions. Allowing for Enterprise Risk Management implementation.
- Provide Windows / Virtual environment vulnerability mitigation and remediation for patching, upgrades and configurations through Group Policy and Regedit for Change Management compliance.

Generate deliverables for quarterly systems/organizational audits for business stance on NIST (RMF) requirements.

- Prepare artifacts, system security plans, security controls traceability matrix, and security concept of operations, to support the Authority to Operate *(ATO).*
- Create and provide guidance towards appropriate artifacts and deliverables: Business Risk Justifications *(BRJ's),* Plan of Action and Milestones *(POA&M's)* and False Positive *(FP)* documentation resulting in 100% auditing completion.
    - Engage Subject Matter Experts *(SME's)* and Application owners, ensuring implementation of technical security controls, verifying controls compliance with key artifacts, deliverables, and requirements towards successful audit completion.
    - Contribute as SME and Technology Owner for Security Configuration Checklists *(SCC),* the organizational version of the Security Technical Implementation Guide *(STIG)* maintaining business related compliance.

Configuring and maintaining physical, VMware and Hyper-V servers within a large Virtual Data Center *(VDC)* achieving NIST / Business RMF compliance.

- Troubleshoot and remediate complex issues and provide root cause analysis for Incident Management process.
- Create server certificate requests, apply for certificate creation from the Certificate Authority *(CA)* for application of SHA2 *(256 bit)* server certificates ensuring accurate Public Key Infrastructure (PKI) compliance.

Sr. System Engineer *02 / 2011 – 03 / 2015*

General Dynamics Information Technology

Sr. System Engineer – Administrator *(07 / 2012 – 03 / 2015)*

General Dynamics Information Technology | PACOM (*Oahu, HI*)

Created, provisioned, and maintained enterprise-level servers and workstations for multiple world-wide classified networks for Department of Defense *(DoD)* in Pacific Command *(PACOM)* achieving NIST RMF compliance.

- Directed daily operations, support, and maintenance of virtual and physical systems/ environments; designed system solutions utilizing SAS, NAS, tape, and SSD resulting in Business Continuity and Disaster Recovery success.
- Configured, implemented, and maintained Symantec Endpoint Manager for Anti-Virus network solutions in LAN/WAN environments; supported multiple hardware platforms and operating systems achieving Endpoint Protection.
- Established WSUS server and performed weekly Microsoft patch updates, including IAVA and 3rd party patches facilitating patch and system management.

System upgrades, documentation, hardware, software, & network troubleshooting. Drove compliance and integrity, adhering to DISA STIG standards when provisioning environments.

Achieved 100% user availability by implementing Windows workstations and servers in physical and VMware virtual clustered environments.

Delivered system automation and reporting verification for security compliance by creating and implementing PowerShell scripts.

Sr. System Engineer – Administrator | Information Assurance Network Officer *(02 / 2011 – 06 / 2012)*

General Dynamics Information Technology | USACE (*Kabul, Afghanistan)*

Served as Information Assurance Network Officer (IANO) and Sr. Systems Engineer / Administrator in virtual and physical Enterprise environments in the Northern Afghanistan Region. Leader of a 16-member Enterprise Service Technologists, providing Tier I, II, and III support, resolving 100% of technical issues.

- Oversaw daily operations, account creations and access control, support, and maintenance for systems, including virtual & physical enterprise environments for United States Army Corps of Engineers *(USACE)* achieving Identity Access Management alignment.
- Managed 9-member project team during Security Encryption and Decryption project to create, deploy, configure, and manage computer encryption methods for Data-at-Rest with Trend Micro Mobile Armor establishing the organizational DAR solution.
- Spearheaded and optimized efforts for 6-member project team for system backup, restoration, archiving, and disaster recovery, ensuring data stability and recoverability for BC/DR efforts.

Sr. System Administrator, *Level IV* *10 / 2010 – 02 / 2011*

Lockheed Martin | DoJ (Washington, D.C.)

Administered the Secure Network Operating Center (NOC) supporting Department of Justice (DoJ) litigation information databases comprised of Windows 2003/2008 and Windows XP, LAN / WAN equipment, anti-virus, and disaster recovery as directed by Enterprise and Information Risk Management.

- Controlled Secure Network Operating Center (NOC) to support Department of Justice's (DoJ) litigation information databases. Managed servers and environments through Active Directory, Group Policy, IIS, RAID configurations, clustered technologies, McAfee's Foundstone insuring alignment with business directives.
- Managed project team to successfully revise and update NIST 800-53 Rev 3 certification & accreditation controls for MEGA-NOC program for civilian litigation in DoJ delivering successful audit compliance.
- Increased speed and performance 35%, analyzing process and implementing SAN backup system with BackupExec upgrade; established de-duplication methods with granular restoration establishing disk-to-disk-to-tape de-duplication methods with granular restoration for "grandfather-to-father-to-son" procedures.

System Engineer – Administrator

08 / 2009 – 08 / 2010

Applied Computing Technologies (ACT) | (Washington, D.C.)

Continual Educational Pursuits

Currently enrolled in the Western Governors University, completing my last year of my Bachelor's Degree for Cloud and Systems Administration.

CISSP, ten-week training class in progress.

Certifications & Technical Expertise

- Certified Information Security Manager (CISM) *(Certification # 1840465)*
- Microsoft Certified Solutions Associate (MCSA): Windows Server 2012 *(Certification # F018-5583)*
- Certified Identity and Access Manager (CIAM) *(Certification # 4239)*
- Microsoft Certified Technology Specialist (MCTS): Windows 7 *(Certification # A762-8759)*
- Microsoft Specialist (MCTS): Windows 7 *(Certification # F4969530)*
- Certificate of Cloud Security Knowledge (CCSK) *(Code: 5gcoMUtyn7Zc40e7zAaRVwiQ)*
- VMware Certified Professional (VCP5-DCV) *(Code: 11374564-91D1-97DC9ED1B49B)*
- Certified Access Management Specialist (CAMS) *(Certification # 4238)*
- Microsoft Certified Professional (MCP): Windows *(Certification # E546-4143)*
- CompTIA Security +; A +; Network +

Operating Systems & Servers:

Windows (XP / 7 / 10), Windows Server (2003 / 2008 / 2012 / 2016), VMware (4.0 / 5.0 / 5.5 / 6.0) VMware vCenter, VMware vMotion, (ESX, ESXi, Hyper-V hypervisors) and Red Hat Enterprise Linux (RHEL), Windows Internet Information Server (IIS), Windows Server Update Services (WSUS)

System Security Assessments/Hardening Tools:

Nessus, Tripwire, STIG Viewer, Active Directory / Group Policy, RegEdit, Symantec Endpoint Protection, Symantec Backup Exec, KACE, SANS 20 Critical Security Controls, Certificate Services - Public Key Infrastructure (PKI)

Key Processes:

Change Management, Incident Management, Endpoint Protection, Vulnerability Assessment, Remediation and Mitigation, Security Documentation, ICMP, DHCP, DNS, HTTP, FTP, VPN

Architectural Tools:

CSA Cloud Control Matrix (CCM), CSA Consensus Assessments Initiative Questionnaire (CAIQ), CSA Star Registry, European Network and Information Security Agency (ENISA) Cloud Computing and Risk Assessment

Organizational Memberships:

CSA Cloud Alliance, Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), International Information Systems Security Certification Consortium (ISC2), United States Computer Emergency Readiness Team (US-CERT), SANS, Dark Reading